"Preventing a Cyber Dresden":

How the Evolution of Air Power can Guide the Evolution of Cyber Power

by

Timothy Neal-Hopes, Wing Commander, Royal Air Force

A thesis submitted to the faculty of the School of Advanced Air and Space Studies for completion of graduation requirements for

School of Advanced Air and Space Studies

Maxwell Air Force Base, Alabama

June 2011

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

_____

Dr. John Sheldon (Date)

_____

Dr. Thomas Hughes (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the UK or US governments, the Ministry of Defence, the Department of Defense, the Royal Air Force, the United States Air Force, or the Air University.

ABOUT THE AUTHOR

Wing Commander Timothy Neal-Hopes is a British officer serving in the Royal Air Force as a Communications and Electronics Engineering specialist. Commissioned in 1994, Wing Commander Neal-Hopes is a graduate of Royal Air Force College Cranwell. His first practical assignment was as the communications and information systems specialist officer at Royal Air Force Coltishall. From there, in 1998, he was deployed to the Falkland Islands as part of a Joint communications and information systems organization. After completing a Masters degree in Computer and Network Security at Essex University, Wing Commander Neal-Hopes returned to Royal Air Force College Cranwell as the Head Information Systems Lecturer where he established the College's malware laboratory and taught network and security design tailored to the military context. Subsequent tours have seen Neal-Hopes serve as Officer Commanding No 1 Expeditionary Radar and Airfield Squadron, supporting operations in Iraq and Afghanistan; and thereafter, as Senior Career Manager for 400 Royal Air Force engineering officers within the Communications Electronics and Avionics specializations. Prior to attending the School of Advanced Air and Space Studies, he was employed in the British Embassy and wider Washington D.C. area as a staff officer responsible for multinational air and cyber power interoperability issues. Wing Commander Neal-Hopes is a graduate of the United Kingdom's Joint Services Command and Staff College. He is married and has one daughter.

ACKNOWLEDGEMENTS

I would like to express my gratitude to Dr. John Sheldon of the School of Advanced Air and Space Studies (SAASS), who has been instrumental in the completion of this study. I must acknowledge the outstanding counsel he has provided throughout the course of this work. His incisive analytical mind is only paralleled by the consummate expertise and experience that he has of the cyber and space security arenas. Not only did Dr Sheldon provide most excellent support and critical advice on the core thesis matter, he has also opened the author's eyes to the perils of strategic analogy and turned me into a schizophrenic disciple of both Sir Michael Howard's school of analytical reasoning; and Martin Van Creveld's school of historical analogy. My opposable mind is thanks to him.

I am also grateful to Dr. Thomas Hughes, also of SAASS, who provided reviews and critiques of my work. His insightful comments on my initial draft were key factors in the completion of this study and I will never forget the first feedback he gave me regarding my work: "Making allowances for the fact you are English, you write well." Sir, may I mirror your sentiments: "For an American, you do not write badly either!"

Though I must also recognize the support and inspiration that I received from all of the professors and my peers from SAASS Class XX, as the author of this work it is my privilege to claim sole responsibility for all the mistakes, factual errors and assertions that this thesis contains. Moreover, for those British readers out there, I promise that a translation will soon follow!

Most importantly, I must thank my wife, and my daughter, for their love and unconditional support during this phenomenal year. The SAASS journey requires more than a student's commitment and masochistic tendencies. My girls have always been there to make me laugh, support me, and keep the important things in life in perspective throughout the completion of this project. With all my love, I dedicate this thesis to them.

ABSTRACT

World Wars I and II witnessed air power's development in the crucible of hostilities. Ambiguous and competing air power schools of thought, on occasion, resulted in the strategically questionable employment of air power. The Allies' bombing of the cultural city of Dresden in February 1945 serves as a vivid instance of the results of these tensions. The firestorms that devastated Dresden now inflame the contemporary air power debate: was the area bombing of Dresden proportionate to the commensurate military gains?

Striking similarities exist between the emergence of cyber power today, as a means of warfare in a new domain, and the development of air power in the first half of the twentieth century. Reflection upon air power's evolution has been employed as a guide for the more efficient and effective development of cyber power. An analysis of air power's formative years has highlighted many of the pitfalls that lie hidden on cyber power's developmental path. An awareness of these pitfalls will allow cyber power to develop pre-emptive strategies on how best to avoid them; thus, debates pertaining to a cyber Dresden will be able to take place before, rather than after, the event.

Learning from air power's early experiences will help prevent cyber power from becoming mired in the same pits that frustrated air power's development. In turn, cyber advocates will be better able to concentrate their focus upon developing a coherent theory of cyber power, uniquely tailored to the challenges of their own domain.

CONTENTS

INTRODUCTION

Not to have an adequate air force in the present state of the world is to compromise the foundations of national freedom and independence.

-- *Winston Churchill*
House of Commons, 14 March 1933.

Government, the private sector and citizens are
under sustained cyber attack today, both from hostile states and criminals.
-- *UK National Security Strategy, 2010.*

The UK, and its closest ally, the US are nations under attack. Paraphrasing the Greatest Briton, not to have an adequate cyber force in the present state of the world would be to compromise the very foundations upon which our nations' freedoms rest. Indeed, such sentiment has become reality. In the case of the UK, fear of not having an adequate cyber force has witnessed the cyber warrior's ascendancy to the status of most favored child: despite significant public spending pressures, £650 million of new investment has been made available in the most recent defense review.[1] In the US, the creation of Cyber Command in 2010 heralded similar recognition of the importance and dependence upon cyberspace.[2] Cyberspace has unquestionably become the growth business in the defense and security marketplace, not only in terms of risk, but now also in terms of resource.[3] But fiscal resource does not equate to an adequate cyber force. Neither does a simplistic focus on force size alone. Clausewitz challenged that "in modern war one will search in vain for a battle in which the winning side triumphed over

---

[1] UK Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: Cabinet Office, 2010), http://www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-defence-security-review.pdf, 47, accessed 21 October 2010.

[2] The US government is expected to spend in excess of $55 billion on cyber defences between 2010 and 2015. Source *US Federal Cybersecurity Market Forecast 2010-2015, Market Research Media*, 5 May 2009, http://www.marketresearchmedia.com/2009/05/25/us-federal-cybersecurity-market-forecast-2010-2015', accessed 25 January 2011.

[3] The 2010 Strategic Defence and Security Review, elevated cyber space to one of only four Tier One risks to the UK's national security.

an army twice its size."[4] Search no longer. The Battle of Britain witnessed the Royal Air Force's defeat of a battle-hardened Luftwaffe that had entered the affray with a two-to-one numerical advantage in terms of first-line aircraft.[5] Ensuring the development of an adequate force, fit to face an onslaught of similar significance in cyberspace today, therefore represents a complex challenge of strategic import for our political and military leaders.

What then does this new-found recognition signify for modern militaries writ large? After all, Defense has long appreciated that, in the Information Age, cyberspace represents the veins through which a successful military's informational lifeblood flows. As Lonsdale noted, information must be regarded as a strategically important asset:[6] be that command and control information to facilitate Van Creveld's "directed telescope";[7] Global Positioning Systems to enable precision targeting of weapons; or logistics support systems to ensure that forces can sustain the fight. Reassuringly, an appreciation of information's widespread importance is already at the heart of current UK and US military doctrine as demonstrated in concepts such as Network Enabled Capability, and Network Centric Warfare. The very essence of these concepts is the efficient routing and pumping of information between the military limbs of sensor and shooter; and ensuring that the decision-making brain does not atrophy because of information-starvation or isolation. As Libicki posited, the circulatory "system of systems" that is cyberspace, can already be argued to represent any advanced military force's center of gravity.[8]

---

[4] Clausewitz conducts a full analysis of the relative strength of opposing military forces in Book 5, Chapter 3 of *On War*. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 282-284.

[5] The Royal Air Force is used in an all-encompassing sense here. In 1940, Fighter Command was a truly international force with twenty percent of its aircrew strength coming from the outstanding contribution of the pilots from the Commonwealth, Continental Europe and the US. For full details of British and German aircraft strength see Stephen Bungay, *The Most Dangerous Enemy* (London: Zenith Press, 2010), 74. Aircrew nationalities and numbers are detailed on 121.

[6] David Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York, NY: Frank Cass, 2004), 11.

[7] Van Creveld introduces the concept of the Commander's "directed telescope" to help thin Clausewitzian fog. Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 75.

[8] Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press. 2007), 1.

What this influx of new resource truly heralds therefore is not a growth in the appreciation of the importance of information or cyberspace, but rather it prophesies an unprecedented period of growth and change: new organizations have already begun to emerge; new policies and strategies to guide the actions of those organizations are being formulated; new doctrine will be developed; and new capabilities and weapons will be created to arm this pioneer generation of cyber warriors. But with such change comes uncertainty, and with uncertainty, risk. The challenge that awaits cyber warriors, and their political masters, is how best to manage the many diverse facets of this growth, and in doing so, reduce the risk that lies therein.

The growth of cyber power up to this point in history can perhaps best be described as a process of emergence and aggregation.[9] Like any emergent process, this has been an inherently non-linear, and bottom-up process. A process in which, as Beech cautions, "leaders do not create a system, but rather are created by it."[10] Emergence unchecked, therefore, can be argued to represent a constraining influence upon leadership and control. The recognition and resourcing of cyber power represents a unique window of opportunity to reverse this emergent dynamic, and for empowered leaders to genuinely shape the development of strategy and capabilities. If this fleeting opportunity is seized, the risk that cyber power's growth represents can in turn be mitigated.

But a challenge that cyber power's leadership must face is that this window of opportunity is fleeting indeed: in the realm of cyber, change is measured in terms of weeks and months, rather than years and decades. Fortunately the challenges associated with the emergence, and growth, of military capability in a new domain are not without precedent. As Sir Winston Churchill's words remind us, both the UK and US have been in this position before. Striking similarities exist between the emergence of cyber power as a means of warfare in a new domain today, and the development of air power that took place in the first half of the twentieth century. The purpose of this report is to apply the familiar and thoroughly-researched development of air power, as a contextual framework to help inform the development of cyber power. It is important to note, however, that

[9] Witness the coming together of existing force elements to create US CYBERCOM.

[10] Michael F Beech, *Observing Al Quaeda Through the Lens of Complexity Theory: Recommendations for the National Strategy to Defeat Terrorism*, Centre for Strategic Leadership, US Army War College, July 2004, http://www.au.af.mil/au/awc/awcgate/army-usawc/csl-quaeda-complex.pdf

reflection upon air power's evolution is not intended to serve as a blueprint for the development of cyber power. Rather, it will be demonstrated that air power can serve as a guide for the more expedient, efficient and effective development of cyber power.

Air power's emergence in the crucible of hostilities borne of World Wars I and II will serve as the historical reference points upon which this study will focus. Herein, critical moments in history were shaped by the successful employment of air power: the Battle of Britain; and more controversially, the UK and US's strategic bombing of Germany and Japan. But on these occasions, ambiguous and competing air power schools of thought also challenged how air power should best be employed. At times, such debates resulted in the strategically questionable employment of air power. For example, the Allies' bombing of the cultural city of Dresden in February 1945 serves as a vivid instance of the results of these tensions. The firestorms that devastated Dresden now inflame the contemporary air power debate: was the area bombing of Dresden proportionate to the commensurate military gains? Many would answer emphatically "No". It is therefore intended that analysis of air power's formative years can highlight many of the pitfalls that lie hidden on cyber power's development path. An awareness of these pitfalls will allow cyber power to develop pre-emptive strategies on how best to avoid its own cyber-Dresden. Moreover, learning from air power's early experiences will also help prevent cyber power from becoming mired in the same debates that frustrated air power's development. By avoiding these unwelcome distractions, leaders will be better able to concentrate their focus upon the priority challenges of today: developing an adequate cyber force to deliver military advantage; and the development of a coherent theory of cyber power, uniquely tailored to the strategic challenges and opportunities that the domain represents.

Before the applicability air power's lessons can be analyzed within the context of cyber power, a solid foundation is required upon which any such analysis can be built. A critical examination of the history and fundamental concepts associated with the Fifth Battlespace that is cyberspace, must therefore lead the way. It will be shown that cyber power, like air power's formative years, has been characterized by soaring advances in technology. Like air power before it, cyber power will continue to develop at a rapid

march and across an exceedingly broad front.[11] A consequence of this conclusion is that any analysis of cyber power must respect its temporally fleeting characteristic: exposure of the strategic pitfalls lie hidden on cyber's path are therefore best exposed by analysis of broader trends in capability development, rather than the tactical details of specific technologies. It will also be argued that the Fifth Battlespace has characteristics that fundamentally differentiate it from its older siblings: land, sea, air and space. At the core of this argument is the fact that cyberspace is the only domain that is, to a significant degree, created by man. Whilst land, air, sea and space were all inherited by mankind, in cyberspace, man is the Creator. It will be demonstrated that the man-made nature of the Fifth Battlespace presents strategists with a paradox: on one hand, the domain is inherently more complex and ethereal than its sister domains because of its dynamic nature; on the other hand, cyberspace's very malleability presents strategists with courses of action that could not be contemplated in the other domains. The complexities of these differentiating characteristics must therefore not be ignored when considering the applicability of air power's lessons to cyber power. Most importantly, it will be argued that any unifying theory of cyber power that serves to guide future strategists must be perpetually re-evaluated in the context of changes in the Fifth Battlespace itself, if it is to remain valid.

Armed with a clear definition and understanding of the cyber domain, this report will then go on to demonstrate why air power is an appropriate lens through which to view the development of cyber power. The validity of historical analogy informing the development of cyber power will first be examined. Whilst air power had World Wars I and II to help inform and shape its development, cyber power has yet to experience Web War I, contrary to the assertions of commentators such as Blank.[12] Van Creveld suggests that military history is the only basis upon which new theory can be built.[13] Whilst this thesis does not agree with Van Creveld's assertion in toto, it will concur that historical analogy is the most suitable lens. Most importantly, historical analogy will provide a

[11] Franklin Kramer, *Cyberpower and National Security* (Washington, DC: National Defense University Press: Potomac Books, 2009), 4.
[12] Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy*, Volume 27, Issue 3, May 2008 , 227–247.
[13] Martin Van Creveld, *Technology and War* (New York: The Free Press, 1989), 278.

mechanism by which cyber power can be broken into its constituent parts for more focused analysis: a weakness that abounds in contemporary cyber thinking, and will be addressed in more detail later in this paper's consideration of the roles of cyber power. As Mark Twain noted, "History does not repeat itself, but it does rhyme." It will be demonstrated that cyber power and air power rhyme in a great many places: the challenges associated with operating in a new domain; the technological demands that must be conquered to turn science fiction into reality; and that cyberspace, like air in its formative years, represents an "imperfect commons" of competing ownership claims, and a deficit of well developed rules.[14] But the power of analogy will be used not just to expose lessons in those areas where air power and cyber power rhyme, but also to highlight dissonance and where the analogy breaks down. In doing so, areas of uncertainty and risk, where cyber must strike its own path, will be more clearly identified.

Having demonstrated the validity of historical analogy as a means by which to help guide cyber power's development, the emergence of the roles of air power, developed in an action-reaction cycle over the trenches of World War I and beyond, demand consideration. An analysis of air power's tasks will provide a prism through which cyber power can be broken into its constituent parts. It will then be shown that the cyber lexicon is woefully inadequate to capture the current and future roles that cyber must play. In an unprecedented era of growth, the consequences of constructing a cyber Tower of Babel will be exposed: reflection upon air power's own muddled taxonomy will ably demonstrate the risks that lie therein. A new framework to better articulate cyber's roles will then be derived. Only by breaking down the problem space that is cyber can priority development areas be identified to facilitate the reversal of the current emergent dynamic.

The development of a framework for a new cyber taxonomy will in turn be utilized as a means by which the perils of competing paradigms within the cyber community can be analyzed and the pitfalls therein exposed. The siren song of air power, and particularly the allure of strategic bombing, will be considered in relation to the

[14] The metaphor is drawn from *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: Center for Strategic International Studies, 2008).

contemporary concept of Strategic Information Warfare.[15] It will be contested that many of the charms that led to Douhet's conclusion that air power represents a "weapon superlatively adapted to offensive operations" resonate with many in the cyber domain today.[16] In stark contrast, Libicki cautioned of the absurdity of building up hostile conquest in cyberspace as strategic.[17] This paper will concur that the charms of Strategic Information Warfare must not be allowed to beguile leaders and strategists to downplay the more pressing demands of defensive, and Joint auxiliary cyber operations. Failure to mitigate this risk may result in the unwary traveler being smashed upon the rocks of strategic failure. Instead, a new paradigm for cyber is demanded: one founded upon a balanced portfolio of defensive, offensive, and auxiliary supporting capabilities. Unlike air power, however, *primus inter pares* of these must be defense.

The strategic portfolio of priorities that leaders are charged with satisfying will then be used to consider issues pertaining to the forging of an adequate cyber force to meet the demands of the present and future state of the world. Air power's eternal debate regarding independence will be drawn upon to demonstrate the dangers that such a diversion represents: a focus upon independence carries with it a significant risk that cyber-leaders may stray from the path of strategic efficacy. In turn, this analysis will be used to demonstrate that a new form of advocacy is demanded for cyberspace. Cyber power's Mitchells and Douhets must be muted: evangelists such as Arquilla, in postulating that control warfare can "achieve victory at a low cost in terms of blood and treasure even against the strongest opponents" present an irresistible dish before politicians whose palate is well suited to such temptations.[18] But as air power's history has proven, such "panaceas" rarely live up to expectation.[19] Advocacy founded not in the realm of information dominance must instead be replaced with the realities of *terra nullius*.

---

[15] The term Strategic Information Warfare was originally coined by Roger C. Molander. See Roger C. Molander, *Strategic Information Warfare: A New Face of War (*Santa Monica, CA: RAND, 1996).
[16] Giulio Douhet, *The Command of the Air* (Tuscaloosa, AL: University of Alabama Press, 2009), 16.
[17] Libicki. *Conquest in Cyberspace: National Security and Information Warfare,* 11.
[18] John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review,* Vol. 22, No. 3, Summer 1994, 25.
[19] Tami Biddle, *Rhetoric and Reality in Air Warfare,* (Princeton, NJ: Princeton University Press, 2004), 248.

Chapter 1

THE FIFTH BATTLESPACE

Cyberspace. A consensual hallucination experienced daily by billions.

-- William Gibson
Neuromancer, 1984.

Dispelling the Consensual Hallucination

Gibson' words were prophetic indeed! Cyberspace is a consensual hallucination experienced daily by billions. The irony is that the hallucination refers not to some Matrix-esque simulated reality, but instead to the very term Gibson first coined. A quarter of a century has passed since cyberspace's first appearance in the science fiction novel *Neuromancer*. Today, cyberspace is a word that springs effortlessly to the lips of presidents, professors and the proletariat alike. The consensual hallucination is that the term rarely means the same thing to any two individuals who utter it. Kramer noted that "cyberspace can be defined in many ways."[1] What is concerning for cyber strategists is that Kramer's words are true.[2] A plethora of definitions for cyberspace abound, and the list continues to grow daily.

Within Defense at least, this hallucination has been recognized, and the perils have started to be addressed. A Cyberspace Operations Lexicon has been issued which is to act as a springboard for normalizing cyber-related terminology.[3] The Lexicon defines cyberspace as a "Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructure."[4] Whilst this definition may provide a normalizing of terminology, this paper suggests that such a definition fails to capture the complexities associated with the unique characteristics of the Fifth Battlespace.

---

[1] Franklin Kramer, *Cyberpower and National Security* (Washington, DC: National Defense University Press: Potomac Books, 2009), 4.

[2] See Dan Kuehl, *From Cyberspace to Cyberpower: Defining the Problem* (National Defense University Press, 2009), 6.

[3] Joint Terminology for Cyberspace Operations, Memo from the Vice Chairman of the Joint Chiefs of Staff, General James Cartwright.

[4] The Lexicon definition contains a typographic error, networkee rather than networked, that has been corrected for the purpose of this paper. *Cyberspace Operations Lexicon*, 7.

First, this paper contests that the definition does not emphasize that cyberspace is, to a significant degree, man-made. As Rattray notes, it is man's electronic creations that shape the electromagnetic battlespace: by allowing entry into it; transmission within it; and use of the information contained therein.[5] Second, the implication of man's role as Creator is that the cyber domain itself will evolve: it is inherently dynamic. Yesterday's radio and television are likely to be but facets of tomorrow's Internet; yesteryear's Corn Exchange is this year's *eBay*. Cyberspace is growing and evolving; a dynamic bounded only by the ungovernable constraints of its Creators' imagination and technological feasibility. The dynamic nature of the cyber domain significantly differentiates it from its siblings: land, sea, air and space. Mahan's sea is still the sea; Douhet's air is still that which we breath; and the land that Napoleon fought for is still inhabited by man today. But cyberspace is fundamentally different: the only guarantee concerning the future of the Fifth Battlespace is that the domain of today will differ from that of tomorrow. Last, this paper contests that the Cyberspace Operations Lexicon fails to emphasize that cyberspace is a domain created and sustained by man, solely driven for the purpose of creating effects in cyberspace or its sister domains. The interrelatedness of cyberspace, with its sister domains, and other instruments of power, therefore demands emphasis.

In a manner reminiscent of Clausewitz, this paper employs an alternative definition of cyberspace that emphasizes a Threefold Order unique to the cyber domain: it is man-made; dynamic; and interrelated.[6] Cyberspace is therefore defined as: "**An *inherently dynamic* layered domain characterized by the *man-made creation and use of electronics* and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructure for the purpose of creating *effects in cyberspace or its sister domains: land, sea, air and space*.**"[7] Only by proffering such a non-reductionist definition are policymakers and cyber strategists presented with the unique paradox that cyberspace presents. On the one hand, the domain is more complex and ethereal than its sister domains because of its dynamic and

[5] Gregory Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 65.
[6] J.F.C. Fuller, *The Foundations of the Science of War*, (London: Hutchinson & Co., 1926), 47.
[7] The concept of cyberspace being layered used here is not in relation to Libicki's physical, syntactic, semantic and pragmatic layers of cyberspace, but rather to highlight that cyberspace is not automatically contiguous. Archipelagoes of strictly-bounded connectivity may exist within the wider domain. Libicki, *Conquest in Cyberspace*, 231-240.

interrelated nature; on the other hand, cyberspace's very malleability presents strategists with courses of action that could not be contemplated in the other domains.[8]

If strategists are to forge an adequate cyber force fit to meet the demands of the domain, the cyber power they are charged to wield must also be understood. Unfortunately, it appears that cyber warriors are already learning the bad habits of history. Just as Douhet failed to define air power, so the concept of cyber power is missing from the Cyberspace Operations Lexicon. This paper will therefore employ Kuehl's definition for the purposes of its analysis: *"**Cyber power is the ability to use cyberspace to create advantages and influence events in the other operating environments and across the instruments of power.**"*[9] The relative nature of cyber power in this definition is important for strategists in the context of developing an adequate cyber force. Adequacy can only be defined by first considering the advantages one wishes to create; and second, by having a clear understanding of whom one wishes to have advantage over. The first question a cyber strategist must ask therefore is: "Who are our key competitors or adversaries?" Moreover, the interrelatedness of cyberspace is also crucial in assessing the adequacy of any cyber force: cyber power is not just employed to produce preferred outcomes in cyberspace. Cyber power is also being wielded to produce outcomes in the domains outside of cyberspace.[10] An examination of the emergence of cyber power will demonstrate that ensuring adequate relative advantage has not been at the forefront of cyberspace's development or employ. Ungoverned leverage of the perceived advantages of cyberspace has resulted in the unwitting creation of vulnerabilities for cyber strategists to contend with. Any utilization of cyberspace not only creates power for oneself, but as will be shown, can also gift cyber power to one's adversaries.

---

[8] Gregory Rattray, *An Environmental Approach to Understanding Cyberpower*, in Kramer, *Cyberpower and National Security*, 256.

[9] Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, 16.

[10] Joseph Nye, *Cyber Power* (Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010), 4.

The Emergence of Cyber Power

"We were making the future and hardly any of us troubled to think what future we were making. And here it is!"

-- *H.G. Wells*

When The Sleeper Wakes, 1899.

Cyberspace has been described as a designed environment, created with the specific intent to increase communication and better leverage information.[11] But the term design implies a far greater degree of control than history suggests. Instead, this paper contests that the growth of cyberspace and its employ, to create cyber power, up to this point in time is better described as a process of emergence and aggregation rather than design. It is ironic therefore that a domain founded upon the transfer of ones and zeros is perhaps more a Darwinian "offspring of history" than a child raised of logic.[12]

In the beginning ARPA created cyberspace.[13] Whilst the invention of the telegraph, telephone, radio, and computer cannot be ignored as stepping stones on the path to the creation of cyberspace, it was the advent of packet-switched networking that truly facilitated the unprecedented integration of these capabilities. The creation of cyberspace therefore cannot be decoupled from Licklider's concept of a Galactic Network. By the end of 1969, that concept had become actuality in the form of the Defense Department's modest connection of four computers called ARPANET. Mankind had created the first operational packet-switched network, invented to increase the resilience and cost-effectiveness of circuit-based switching.[14] In the beginning there had been control: cyberspace had been a designed and bounded environment. But then cyberspace changed. Control was surrendered and emergence reigned.[15]

---

[11] Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, 29.

[12] The term offspring of history is drawn from Stephen Jay Gould, *Rocks of Ages: Science and Religion in the Fullness of Life* (New York: Ballantine, 1999), 191.

[13] Advanced Research Projects Agency (ARPA) changed its name to Defense Advanced Research Projects Agency (DARPA) in 1971, then back to ARPA in 1993, and back to DARPA in 1996. The wheel of change turns quickly!

[14] Barry Leiner et al, *A Brief History of the Internet*, http://www.isoc.org/internet/history/brief.shtml

[15] Robert Kahn wrote four "Ground Rules" to develop the open-architecture networked environment that would shape the evolution of internetworking. Rule Four states: "There would be no global control at the operations level." Robert Kahn and Vinton Cerf invented the Transmission Control Protocol (TCP) and the

Kahn and Cerf's invention of the communication protocols TCP/IP, founded upon the principle that there would be no global control, sealed cyberspace's fate as an anarchic realm. The implications would prove most significant. To explain, a brief examination of another anarchic realm, the international system, is prudent. Waltz's seminal *Theory of International Politics* described the international system as one of self-help: the absence of any governing order, higher than the state itself, demands that states must conduct their affairs in the "brooding shadow of violence."[16] At any time, one state may elect to use force. Consequently, all states must be prepared to do so, or live at the mercy of their neighbors. This paper suggests that a parallel exists with cyberspace today: the absence of a pan-cyberspace governing order means that a "brooding shadow of violence" hangs over all residents of the global village.[17] In cyberspace, states must therefore remain ever-ready to defend themselves with force as necessary unless they are prepared to live at the mercy of their neighbors. For a Realist, an anarchic cyberspace must first, and foremost, be viewed as the Fifth Battlespace. Unfortunately for the UK and the US, the implications of the anarchic nature of cyberspace were not immediately realized. The result, as shall be demonstrated, is that the cyber power of both states emerged in an unbalanced fashion.[18]

Emergence and aggregation allowed the original ARPANET, coupled with the introduction of TCP/IP, to evolve into the most recognized facet of cyberspace today: the Internet. The Internet was based on the principle that independent networks could be easily aggregated together; an absence of a pan-cyberspace governing order allowed new applications, protocols and connections to emerge. New applications, protocols and connections that the US and UK would soon become dependent upon in their efforts to employ cyber power to create advantages and opportunities for their other instruments of power: most notably economic growth. The dynamic nature of cyberspace, bounded only by the ungovernable constraints of its Creators' imagination and technological feasibility, is most apparent in this emergent development. Creators such as Tim Berners-Lee, and

---

Internet Protocol (IP) in 1972. TCP/IP remain the fundamental networking and communication protocols upon which all internets are built.

[16] Kenneth Waltz, *Theory of International Politics* (Boston, MA: McGraw Hill, 1979), 104.

[17] Waltz, *Theory of International Politics*, 102.

[18] Mark Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law & Policy*, Volume 4, Number 1, 2010, 173.

Bill Gates, provided the imagination.[19] Moore's Law and Metcalfe's Law describe the technological feasibility: bringing lower cost computing to the masses; and flexible networking connectivity.[20] The offspring of this coupling has been the ever more pervasive, yet ungoverned, expansion of cyberspace. In 1992, there were a million users on the Internet; fifteen years later the number of computers and Internet connections had grown to well over a billion.[21] Cyberspace had expanded to touch upon more and more aspects of daily life for the majority of the world.[22] The acquisition of economic power had proved to be an irresistible catalyst for cyberspace's growth. Businesses re-engineered their processes to take advantage of cyberspace: to shift production, supply chains and sales; gain access to new markets; streamline their practices; and weave an increasingly interrelated and complex geo-economic web.

Influential strategists such Edward Luttwak, and Third Wave economists including Lester Thurow, were keen advocates of this progress, suggesting that economic competition would replace military conflict.[23] The growth of cyber power, fueling economic growth, was therefore only to be applauded. Unfortunately, geo-economic conflict is not a substitute for military conflict. Indeed, economic competition has often been shown to serve as a prelude to military war.[24] Relative advantage in economic growth had been the catalyst of cyberspace's development and employ. But ungoverned pursuit of this advantage had resulted in the unwitting creation of vulnerabilities. Alvin

---

[19] Tim Berners-Lee is credited with the creation of the World Wide Web in 1990. The event was marked by the first successful communication between an Hypertext Transfer Protocol (HTTP) client and server, established via the Internet. Bill Gates, co-founder of Microsoft, has been hugely influential in bringing computing to the masses: first, the creation of PC-DOS for IBM; and, most notably thereafter, the launch of Windows in 1985.

[20] Moore's Law describes that the number of microcomponents that can be etched on a chip will double at regular intervals: two years is the widely accepted interval. Metcalfe's Law posits that the value of a telecommunications network is proportional to the square of the number of its users. Whilst Metcalfe's Law has been challenged, it is generally agreed that the value of a network does grow at a non-linear rate, greater than the number of users. Bob Briscoe, "Metcalfe's Law is Wrong," *IEEE Spectrum*, July 2006.

[21] Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in Kramer, *Cyberpower and National Security*. 52.

[22] Edward Skoudis, "Evolutionary Trends in Cyberspace," in Kramer, *Cyberpower and National Security*, 148.

[23] Edward Luttwak, "Economic Competition Will Replace Military Conflict: From Geopolitics to Geo-Economics," *National Interest*, Summer 1990, 20.

[24] A counter-argument to Luttwak is presented by Elliot Cohen in "The Future of Force," *The National Interest*, Autumn 1990.

and Heidi Toffler exposed the imbalance in the UK and US cyber power equation in their observation that the way states make war reflects the way that they make wealth.[25] This observation has two significant implications upon the military facet of cyber power. First, the advantage that information conveyed to business also began to be emphasized in the business of warfare. As Admiral Cebrowski wrote: "The underlying economics and technologies have changed. American business has changed. We should be surprised and shocked if America's military did not."[26] Consequently, doctrines to reflect this new era of warfare, such as Network Enabled Capability (NEC) in the UK, and its US contemporary, Network-Centric Warfare (NCW) were born. Second, a realization had dawned that the creation of economic power, founded upon an emergent dependence upon cyberspace, demanded that the security of cyberspace must be protected. As Nye reflected, the UK and US governments had been slow to develop serious national plans for cyber security and cyber forces.[27] The wheel of cyberspace had turned: ARPA's baby had become a Defense issue once again.

Cyber Power - A New Theory of Warfare

NEC and NCW were not introduced as mere evolutions in military doctrine. Their champions hailed cyberspace and networks as a revolution in military affairs unlike any witnessed since the Napoleonic Age.[28] Nothing less than a new Tofflerian theory of war was being proposed.[29] Information had facilitated the creation of geo-economic power. Ipso facto, information would enhance the UK and US's overall military power through the creation and leveraging of cyber power: the linking of "sensors, decision-makers, weapon systems and support capability to achieve enhanced military effect through improved exploitation of information."[30] NCW placed great emphasis upon

---

[25] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown and Company, 1993). 3.

[26] Arthur Cebrowski and John Garstka, "Network-Centric Warfare: Its Origin and Future", *Proceedings*, US Naval Institute, January 1998, 1.

[27] "The US government only began to develop serious national plans for cyber security in the past decade." Nye, *Cyber Power*, 4.

[28] P W Singer, *Wired for War* (New York: Penguin, 2009), 181.

[29] "What we are really talking about is a new theory of war because we are talking about new sources of power." Vice Admiral Arthur Cebrowski, Speech to the Network-Centric Warfare Conference, 22 January 2003.

[30] Andrew James, *Understanding Network Enabled Capability* (London: Ministry of Defence, 2009), 12.

increased shared awareness, increased speed of command and a resultant higher tempo of operations.[31] Clausewitz's "fog of war" would be lifted; Boyd's Observe-Orient-Decide-Act (OODA) loop would disappear.[32] These were heady claims indeed, and the dangers of such unadulterated advocacy will be considered later in this paper. But for NEC and NCW, what these new theories of war seemed to miss was that lifting the fog of war would do nothing to dispel the "brooding shadow of violence" that would still hang over the anarchic Fifth Battlespace.

Like business before it, NEC and NCW stimulated the emergence of an increasingly interrelated and complex web of military connectivity. Alberts and Hayes celebrated this process, foretelling that the magic of NCW would enable a leap from shared awareness to self-synchronization, achieved by emergence.[33] In stark contrast, a more cautious school of thought, typified by Kolanda and Roman, warned of the limited transformational effects that NCW and NEC would achieve.[34] The latter school argued that greater connectivity would not stimulate self-synchronization, resilience, and empower the edge of the battlefield. Instead, it would facilitate the military's predominant historic predilection towards greater centralized control and more rigid hierarchical organization. History, thus far, would seem to demonstrate that rigid military hierarchies are alive and well in the Information Age.[35]

ARPANET had been created to provide resilience. Sadly, the first lesson of the Information Age seems to have been forgotten all too soon. If NEC and NCW have reinforced hierarchies, whilst at the same time exposed key processes to attack, resilience

---

[31] NCW is defined as "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability; and a degree of self-synchronization." David Alberts, John Gartska, and Frederick Stein, *Network-Centric Warfare. Developing and Leveraging Information Superiority* (Washington D.C.: Library of Congress, 1999), 2.

[32] Cebrowski, *Network-Centric Warfare: Its Origin and Future*, 6.

[33] David Alberts and Richard Hayes, *Power to the Edge: Command and Control in the Information Age*, (Washington D.C.: Library of Congress, 2003), 208-209.

[34] Christopher Kolanda, "Transforming How We Fight – A Conceptual Approach," *Naval War College Review*, Spring 2003; Gregory Roman, *The Command or Control Dilemma: When Technology and Organizational Orientation Collide*, April, 1996. Available at: http://csat.au.af.mil/2025/volume1/vol1ch04.pdf accessed 18 November 2010.

[35] Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 234.

has been undermined. Like the UK and US business world before it, military transformation had succumbed to the allure of cyber power. Moreover, it has done so in an unbalanced fashion. NEC and NCW have focused overly upon the creation of relative advantage, without giving due regard for the risks inherent in an emergent and ungoverned dynamic. This has resulted in the unwitting creation of vulnerabilities, and granted opportunities for our adversaries to leverage cyber power against us. As General Chilton recently noted, the ability of other states' "cyber warriors to attack and gain entry to military networks is a potential vulnerability of NEC."[36] Cyberspace and networks may well represent the greatest revolution in military affairs since Napoleon, but as the Little Corporal understood so well, it is recognition of the limitations of technology at one's disposal, rather than being shaped by the methods available, that is crucial in seeking out a path to military success.[37]

Before cyber strategists can coherently redress the imbalance that has been created in the UK and US's cyber power, this paper suggests that the question of what vulnerabilities have emerged must first be answered. A brief analysis of the three most significant military skirmishes that have occurred in cyberspace are therefore considered next: Estonia; Georgia; and Iran.

Has Cyberwar Arrived?

In a fashion reminiscent of General Spaatz's warning that the "next war will be preponderantly an air war,"[38] half a century later Arquilla and Ronfeldt emphatically proclaimed: "Cyberwar is coming!"[39] But what is this cyberwar of which they cry? Arquilla and Ronfeldt's concept of cyberwar is neither built upon attritional mass, nor maneuverist mobility. Instead, they declared that information will become king.[40] Like their fellow NEC and NCW advocates, they contest that future conflicts will be fought

[36] What is perhaps more concerning is that in an 82-page document, the vulnerabilities associated with NEC are only discussed twice. John Mulberry, *Network Enabled Capability)*, 79.
[37] Van Creveld, *Command in War*, 188.
[38] David MacIsaac, "The Air Force and Strategic Thought 1945 – 1951", Working Paper #8, *Woodrow Wilson International Center for Scholars*, International Security Studies Program, 1979, 10.
[39] John Arquilla and David Ronfeldt, *Cyberwar is Coming!*, (RAND, 1997).
[40] Arquilla and Ronfeldt's study provides a useful delineation for considering cyber power issues: cyberwar and netwar. Cyberwar refers purely to state-on-state military information-related conflict; netwar refers to broader non-military cyber issues including non-state actors such as terrorists, and organized crime syndicates. This delineation will be drawn upon later in this paper when considering the military roles of cyber power.

more by networks than by hierarchies: whichever adversary masters the network form will gain military advantage. Military success will therefore be conferred to the belligerent who knows more; can disperse the fog of war; and enshroud an adversary in their own fog. Whilst they dangle the allure of savings in blood and treasure before politicians and military strategists alike, cyberspace is merely presented as an extension of the battlefield into the Fifth Battlespace, augmenting rather than replacing its four sister domains.

At the other end of the spectrum, some commentators view cyberwar as challenging the very nature of war itself. Richard Clarke declared: "cyberwar is a wholly new form of combat"; [41] the result is that war fighting will be "forever changed"; and such a change may witness "a shift in the world military balance."[42] On 26th April 2007, events in Estonia led some commentators to conclude that Arquilla and Ronfeldt's prediction had come to pass: Web War I had arrived."[43] NCW's and Clarke's visions bookend a spectrum of possibilities of what cyberwar might look like. Do the events in Estonia fall within this range?

The cyber attacks on Estonia have been heralded by some as an act of war with the intent to create mass social panic.[44] The moving of the now-famed Bronze Soldier provoked a cyberspace assault in the form of distributed denial of service (DDOS) attacks undertaken by botnets targeted at government email systems; some government websites were defaced; and Estonia's two largest banks were forced to take their services temporarily off-line as a precautionary measure.[45] Blank contests these attacks represent war, citing Clausewitz's "clash of wills, where one side attempts to compel the other side to do its will."[46] But Clausewitz stated that the essence of war is fighting: the trial of

---

[41] Richard Clarke, "War from Cyberspace," *The National Interest,* November-December 2009 http://nationalinterest.org/article/war-from-cyberspace-3278 accessed 11 January 2010.
[42] Richard Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 30-32.
[43] Blank, *Web War I: Is Europe's First Information War a New Kind of War?*, 227.
[44] Dennis Murphy, "Attack or Defend? Leveraging Information and Balancing risk in Cyberspace", *Military Review*, May–June 2010, 91.
[45] More details of the cyber-assault against Estonia are available at: Rebecca Grant, *Victory in Cyberspace*, http://www.afa.org/media/reports/victorycyberspace.pdf accessed 10 December 2010.
[46] Blank, *Web War I: Is Europe's First Information War a New Kind of War?*, 4.

moral *and* physical forces through the medium of the latter.[47] A clash of wills alone is but one half of the equation. Considered from an NCW-perspective, Estonia was not enshrouded in a fog of war, laid bare to military assault. Neither did Estonia demonstrate Clarke's vision of military cyber power wreaking devastating consequences in the physical realm. To describe Estonia as cyberwar is therefore to misunderstand the nature of war itself. The lesson that Estonia hints at is the danger inherent in developing an imbalance in cyber power: the emergence of an information dependent society, created without sufficient regard of the vulnerabilities created, or resilience to dull the effects of any assault.[48]

What then of Georgia? In August 2008, as Russian tanks rolled into South Ossetia, presidential, governmental, news and financial websites fell victim to an army of botnets conducting concerted DDOS attacks.[49] Georgia certainly represents one of the first cases in which a military conflict has been coordinated with a cyber offensive.[50] The botnet attacks were crafted to directly support Russian state policy; and timed to inhibit information flow from the Georgian government to both the international public and its own residents.[51] Overall, the effects were far from devastating; however, cyber power was employed as a strategic force multiplier to induce a Clausewitzian fog of war.[52] Moreover, it also represented a trial of both moral and physical forces. To that end, Georgia could be described as a very minor NCW-esque cyber war: cyber power was

---

[47] Clausewitz, *On War*, 127.

[48] It should be noted that Estonia, at the time of the attacks, possessed a number of independently-routed high-capacity fiber links to several countries. These links were owned by several network operators. Moreover, there were binding agreements in place between these operators to enable excess traffic to be diverted.

[49] Eleanor Keymour, "The Cyber-war," *Jane's Defence Weekly*, 2009, Vol 47, Issue 39, 20-24.

[50] For further details of the Georgia case see Eneken Tikk, *Cyber Attacks Against Georgia – Legal Lessons Identified* (CCDCOE, 2008), 4-17. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf accessed 21 December 2010.

[51] Some authors have described the Georgia attacks as "severing" communications with the populace or creating an information vacuum. This is a gross overstatement. For example, see James Farwell, "Stuxnet and the Future of Cyber War," *Survival*, Vol 53, No 1, February-March 2011, 26. It should be noted traditional media avenues including TV and radio remained. Moreover, only 8% of the Georgian populace were Internet users in 2008. In contrast, 66% of Estonians in 2007 had Internet access. For data source visit: *Internet Users per 100 Population, 2007 and 2008*. Available at: http://data.un.org/Data.aspx?q=internet&d=ITU&f=ind1Code%3aI99H accessed 20 January 2011.

[52] Jose Nazario, *Georgia DDoS Attacks: A Quick Summary of Observations* Available at: http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/ accessed 3 December 2010.

employed as an auxiliary means to augment military effect in the land domain; and the political instrument in terms of strategic communications. Most notably, Georgia represents the emergence of how military cyber power can play a role as part of a coordinated military campaign with its sister domains; rather than as a stand-alone means of conducting war.

Estonia and Georgia demonstrate one emerging pattern in military cyber power: the use of botnets against non-military targets, synchronized with political and military action in the physical domain, to induce a fog of war upon one's adversary. Stuxnet represents not only a very different pattern, but also the dynamic nature of threats in the cyber domain.

In June 2010, the world learned that the Iranian nuclear facility at Natanz had been attacked. But this was not a surprise Israeli air strike resembling the attacks against Iraq in June 1981; or Syria in September 2007. Cyber power had supplanted air power. Stuxnet was the weapon; centrifuges, within the hardened fuel enrichment plant at Natanz, were the target.[53] The Stuxnet worm demonstrated the non-linear dynamic of cyber power: an evolutionary leap from a botnet flash mob; to a search and destroy military mission. Stuxnet had been designed to seek out specific frequency-convertor drives, the type of which is employed to control motors in Iran's uranium enrichment centrifuges. The worm, by covertly altering motors' speeds, sabotaged the enrichment process and whilst the precise effects of Stuxnet are likely to remain shrouded in secrecy, a 23% decline in the number of operating Iranian centrifuges has been suggested.[54] Stuxnet, rather than resembling NCW's model of cyberwar, is more closely aligned to Clarke's predictions of a new form of combat targeted against industrial SCADA systems.[55] An isolated network had been attacked; at less political and economic cost that using air power; at zero cost in terms of casualties; and both secret and known centrifuges alike would be vulnerable. Stuxnet represents a potential evolutionary

---

[53] Mark Clayton, 'Stuxnet Malware is Weapon', Christian Science Monitor, http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant accessed 10 December 2010.

[54] McMillian, "Siemens: Stuxnet Worm Hit Industrial Systems," *Computerworld*, 14 September 2010.

[55] For a detailed report on Supervisory Control and Data Acquisition (SCADA) vulnerabilities in target sets including Air Traffic Control systems, electrical generators, train signaling systems, and oil and gas pipelines, see Rose Tsang, Cyberthreats, Vulnerabilities and Attacks on SCADA Networks, available at http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf accessed 22 December 2010.

advancement of cyberwar. An evolution in malware's sophistication, but more importantly, an evolution in military cyber power thinking. Stuxnet had been designed with a specific effect and adversary in mind; cyber power's interrelatedness with the physical domain had been well crafted. Unfortunately, the illusion of control in the anarchic Fifth Battlespace still remained for a number of reasons.

First, Stuxnet ably exposed the risk of collateral damage that military cyber power presents: over 60,000 computers were infected with the Stuxent worm; 40% of which were outside Iran; one of which was an Indian satellite controller.[56] Such collateral damage could gift significant soft power to a potential adversary. Moreover, Stuxnet exposed four day-zero exploits to the world that could now be employed against UK and US systems: a degree of cyber power has been gifted to future adversaries. Last, Stuxnet potentially served to validate the perception that civilian and industrial infrastructure represents a legitimate military target in any future cyber conflict. If accepted, the implications for the UK and US could be grave indeed.

Summary

A critical examination of the history and fundamental concepts of the Fifth Battlespace has been conducted, and an argument presented that cyberspace still represents a conceptual hallucination in terms of shared understanding. Political leaders, military strategists and practitioners all have differing perceptions of what actually constitutes cyberspace and cyber power. Definitions that emphasize the unique Threefold Order of the cyber domain have therefore been proffered as a foundation upon which a more coherent cyber lexicon can be built.

The emergence of cyber power has also been examined and the Fifth Battlespace has been presented as an anarchic domain over which the brooding shadow of violence casts its pall. It has been contested that cyber power's emergence to date has been a largely ungoverned, bottom-up process in which military considerations have often been an afterthought. The result is that cyber power has developed in an unbalanced fashion. Whist the Information Age has created potential economic and military power for the UK

---

[56] James Farwell, "Stuxnet and the Future of Cyber War, *Survival: Global Politics and Strategy*, Vol 53, No 1, February–March 2011, 34.

and US, it has also created vulnerabilities and in so doing, it has gifted a most capable weapon to our adversaries.

Last, it has been shown that conflict in the cyber realm, akin to air power throughout its own history, has been characterized by soaring advances in technology, and bounding leaps in capability. Moreover, the man-made nature of the cyber domain is likely to witness the character of conflict in the cyber domain evolve at an extremely rapid rate, and across an exceedingly broad front. Conflict in cyberspace has already been shown to be here: Estonia, Georgia and Iran have all served as useful calls-to-arms. ARPA's baby has become a matter of military import once again. Most importantly, for the purposes of this thesis, all three of these cyber skirmishes have served to demonstrate the allure of civilian targets to cyber attack. But if, as has been argued, cyberspace is a unique domain, is it valid to employ historic analogy to help guide its future?

Chapter 2

LOOKING THROUGH THE LENS OF AIR POWER

I do not myself believe in any simple 'lessons of history', and I have learned to mistrust historical analogy as a lazy substitute for analytical thought.

-- Sir Michael Howard

History does not repeat itself, but it does rhyme.

-- Mark Twain

Military history can tell us how, in the past, people coped with problems which in some way resembled our own.

-- Martin Van Creveld [1]

The anarchic Fifth Battlespace has been presented as a unique domain, into which future wars will certainly spill. Indeed, conflict in cyberspace has already been shown to be here! But, if cyberspace is a unique domain, is it valid to employ strategic and historic analogy? Will turning the lens of air power's experience upon cyber power create a more balanced capability portfolio in the cyber domain? Sir Michael Howard cautions of the perils inherent in any such comparison. His counsel, that analogy must never be allowed to substitute for analytical thought, is first-rate: an absence of analysis would indeed represent an abdication of responsibility, and any cyber strategy derived in such a manner would be untrustworthy. But the perils of analogy do not equate to the delivery of theoretical perfection via its main rival methodology: inductive reasoning.

Despite cyberspace's immaturity, initial efforts to develop a theory of cyber power via inductive means have been attempted.[2] All have failed to satisfy.[3] As Starr concludes, early attempts to develop a theory for any discipline are inherently "somewhat wrong."[4] Winton goes further in his description of theory as an "imperfect jewel," stating that no theory will ever be complete, and theories are always fated to be somewhat wrong.[5] By its very nature, a theory lags behind contemporary developments in the

---

[1] Martin Van Creveld, *Technology and War,* (New York: The Free Press, 1989), 278.

[2] Harold Winton posits that a theory of warfare should perform five functions if it is to have utility. It must define, categorize, explain, connect, and anticipate the field of study under investigation. Harold Winton, *An Imperfect Jewel: Military Theory and the Military Profession*, 600 Reader.

[3] Starr, *Toward a Preliminary Theory of Cyberpower*, 43-87.

[4] Starr, *Toward a Preliminary Theory of Cyberpower*, 44.

[5] Winton, *An Imperfect Jewel: Military Theory and the Military Profession,* 4.

discipline it seeks to describe. A relationship therefore exists between the rate of change a discipline experiences, and the degree of accuracy that can be expected in any theory. Such a conclusion explains the absence of a satisfactory inductive theory of cyber power to date. Moreover, the exponential rate of change that the cyber discipline will experience in this forthcoming period of unprecedented growth, coupled with the dynamic nature of the cyber domain itself, will present a significant obstacle to the realization of any inductive theory in the immediate future.

If early attempts at inductive reasoning tend to produce theories that are significantly flawed; and, if Howard is to be believed that the path of analogy only represents a lazy substitute for analytical thought, is it not better to abandon both paths and seek an alternative means? This paper suggests not. Strategies that are driven by technology or circumstance, without the integrating factor of a coherent vision, are in reality no strategy at all. Strategy, as Liddell Hart described, is the calculation and co-ordination of military means with political ends.[6] It is a proactive discipline. Any plan that subordinates strategy to another field such as technology, sociology or economics, is reactive. As Dolman rightly notes, willing abandonment of strategic foresight is only likely to be rewarded with failure.[7]

Why Strategic and Historical Analogy Represent a Valid Approach

Hindsight will never grant twenty-twenty foresight, but as Martin Van Creveld posits, military history is the only basis upon which new theory can be built.[8] Unfortunately, Van Creveld's words present a challenge for cyber strategists. Whilst air power had World Wars I and II to help inform and shape its development, it has been demonstrated that cyber power is still in its infancy in terms of experience. The cyber skirmishes of Estonia, Georgia and Iran provide glimpses of aspects of cyber power, but analysis of these incidents alone would be as untrustworthy as Howard's absence of analytical scrutiny. Mark Twain's oft quoted observation that "history rhymes" therefore offers the possibility of a solution: air power's history may rhyme with cyber power's future. An analogical framework that blends strategic and historical approaches must

[6] "Strategy depends for success, first and most, on a sound calculation and coordination of the end and the means." Basil Liddell Hart, *Strategy* (London: Faber & Faber, 1967), 322.
[7] Everett C Dolman, *Astropolitik* (New York: Frank Cass, 2002), 148.
[8] Van Creveld, *Technology and War*, 278.

therefore first be developed. Thereafter, the question of whether airpower is the appropriate lens to apply to cyber power's development must be addressed. Khong cautions that the most obvious analogies often tend to be the most superficial.[9] Consequently, an examination of air power's early development, in relation to cyber power, is demanded to demonstrate that the similarities between the domains go beyond the superficial. It will be shown that air power's development provides a useful proxy to substitute for the relative void in cyber power's experience. Last, the limits of analogy must be iterated to ensure that all lessons drawn from air power are appropriately utilized. It will be demonstrated that air power's experience is best employed to derive warning signs on the path of military cyber power development, rather than as a map to dogmatically follow. Analogical reasoning, whilst useful, is inherently limited and the methodology adopted in this paper does not represent the path to a theory of cyber power: as cyber power's rate of growth slows, and as its experience base expands, the cyber domain will be better placed to develop its own inductive theories and a robust theory of cyber power.

An Analytical Framework

This paper has suggested that a guarded use of analogy provides a short-term risk management strategy for the proactive development of cyber power. A framework to bound the problem space and avoid the perils of analogical reasoning is therefore demanded. Libicki stated that "attempts to transfer policy constructs from other forms of warfare will not only fail but hinder policy and planning."[10] Whilst this assertion is correct, this paper suggests that Libicki is not describing strategic analogical reasoning, but rather strategic plagiarism! Strategic analogy compares the strategic experiences and theories of one domain to another. If it can be demonstrated that the two domains are similar in one respect, critical analysis can be conducted to examine whether they are similar in other respects: Klein's derivation of concepts and principles of space warfare, drawn from Sir Julian Corbett's principles of maritime strategy presents an excellent example of such an approach.[11]

---

[9] Yueng Fhoong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu and the Vietnam Decision of 1965* (Princeton, NJ: Princeton University Press, 1992), 12.
[10] Martin Libicki, *Cyberdeterrence and Cyberwar*,(Santa Monica, CA: RAND, 2009), xiii.
[11] John Klein, *Space Warfare: Strategy, Principles and Policy*, (New York, NY: Routledge, 2006), 21-154.

But strategy is a vast and complex problem-space and a macro-level framework to decompose this space is demanded, both to bound this study, and to ensure that the analysis is being conducted in a fair and methodical fashion. Gray's seminal work *Modern Strategy* will be employed for this purpose. Gray identified seventeen dimensions of strategy, sub-divided into three categories. A comparison of all seventeen dimensions would suffer from the law of diminishing returns. Consequently, the most pertinent of Gray's strategic dimensions, those in which cyber power must make its major decisions, have been selected for detailed scrutiny. To ensure a balanced analysis, dimensions have been chosen from across Gray's categories: the dimension of military operations will be employed to compare the roles of air power and cyber power; the dimension of strategic theory and doctrine will be examined to consider the emergence of air power's competing schools of thought; and the dimension of organization will be considered to expose the challenges that air power faced in its path to independence.[12]

Historical analogy suggests that if two events separated in time agree in one respect, they may agree in another. An outstanding exposé of the use of historical analogy in US policy decision-making is demonstrated in Khong's *Analogies at War*.[13] Khong developed an Analogical Explanation (AE) Framework to tease out micro-level lessons from analogy. The AE Framework is composed of six diagnostic tasks: define the nature of the problem; identify the stakes involved; create a list of possible solutions; evaluate the potential solutions; assess their moral rightness; and warn of any dangers associated. This paper will blend Khong and Gray's approaches in a single framework: each of the three selected strategic dimensions will be analyzed in terms of Khong's six distinct, but related stages. In adopting such an approach, the power and versatility of strategic and historical analogy will applied in an analytically balanced and rigorous

[12] Colin Gray's seventeen dimensions of strategy are sub-divided into three categories: People and Politics; Preparation for War; and War Proper. The category People and Politics contains the dimensions: People; Society; Culture; Politics; and Ethics. Preparation for War includes the dimensions: Economics and Logistics; Organization; Military Administration; Information and Intelligence; Strategic Theory and Doctrine; and Technology. War Proper includes: Military Operations; Command; Geography; Friction, Chance and Uncertainty; Adversary; and Time. For a more detailed description of these dimensions see: Colin Gray, *Modern Strategy*, (New York, NY: Oxford University Press, 1999), 16-44.

[13] Khong, *Analogies at War: Korea, Munich, Dien Bien Phu and the Vietnam Decision of 1965*, 7-8.

manner.[14] Such a methodology will ensure that this paper's analogical analysis is not simply a confirmatory process of the path that cyber power should take. More importantly, it represents a means by which options on the path of cyber power's development can be discounted.

Selecting the Correct Analogy

Skeptics of analogical reasoning challenge that analogies are often used poorly and indiscriminately. In short, strategists and policymakers pick and apply the wrong analogies.[15] The consequences of striking the wrong analogy can be disastrous. For example, British Prime Minister Anthony Eden compared Egypt's seizure of the Suez Canal with Hitler's expansionist intentions for Nazi world dominion: "I surveyed the scene in these autumn months of 1956, and was determined that the like should not come again."[16] This poorly applied analogy fuelled Eden's humiliating folly of retaking the Suez by force. The most obvious analogy did indeed prove to be the most superficial; poor strategy was the result. It is therefore beholden upon this paper to ensure that the most appropriate analogy for the development of cyber power is selected. Three areas of comparison will be considered to verify the validity of air power's experience as a proxy to guide the evolution of cyber power. First, the military exploitation of a new battlespace will be examined; second, the technical nature and demands of both domains will then be analyzed; last, the fuzzy boundaries that characterize the cyber and air domains will be considered.

The Challenge of a New Domain

The famed events at Kitty Hawk on 17 December 1903 did not just herald the invention of the airplane.[17] The Wright brothers' Flyer had conquered a new domain.[18] Controlled flight in a heavier-than-air, man-carrying craft represented mastery over the air domain: a new domain that would soon be employed for the purposes of war-fighting.

---

[14] Employing a framework as proposed also reduces the chance of absurd, holistic and multiple analogical reasoning errors.

[15] Ernest May, *Lessons of the Past; the Use and Misuse of History in American Foreign Policy* (New York, NY: Oxford University Press, 1973), xii.

[16] Anthony Eden, *Full Circle* (Boston, MA: Houghton Mifflin, 1960), 578.

[17] Peter L Jakab, *Visions of a Flying Machine: The Wright Brothers and the Process of Invention* (Washington D.C.: Smithsonian Press, 1990), 211.

[18] It is acknowledged that kites, gliders, dirigibles and balloons had flown before 1903; however, the most enduring artifact of air power is unquestionably the airplane.

Less than two decades would pass before air power advocates, led by Douhet, Mitchell and Trenchard, would devote unprecedented attention upon how future wars could be fought in and from the air. The air itself had not changed, but the domain's strategic utility as a military battlespace had exponentially increased with the advent of the airplane.

Unlike the air, cyberspace has not always been there. It has been shown that cyberspace did not exist before ARPA's first steps to actualize Licklider's concept of a Galactic Network. This difference is made at the outset to highlight the fallacy of seeking perfect analogy. As Fischer observes, a "perfect analogy" is a contradiction in terms.[19] Perfect symmetry between the air and cyber domains is not demanded, or even credible, for the analogy to have utility. It is similarity beyond the superficial that is sought: the major characteristics that influenced air power's development, if present in the cyber domain, demonstrate the analogy's value to help guide cyber power's growth.

Just as the airplane represented an exponential increase in the strategic utility of air as a battlespace, so the emergent expansion of information systems and networks, to the point of near-ubiquity, witnessed the realization of cyber space as a domain of growing strategic utility. For air power, images of Gothas over London kindled the people's passions for war in the air; the offensive utility of air power inflamed the imagination of military commanders;[20] and the allure that air power offered the business of government proved irresistible. [21] Similarly, it is recognition of the Fifth Battlespace, by all members of the Clausewitzian triumvirate, as an accepted new domain of war that mirrors the growth of cyberspace's elder sibling. Douhet recognized that the air domain represented a battlefield limited only by the boundaries of the nations at war: the technical development of aviation made armies and navies irrelevant to the provision of defense against any determined enemy armed with the ability to strike at the heart of a

[19] David Hackett Fischer, *Historians' Fallacies: Toward a Logic of Historical Thought* (New York: Harper Torchbooks, 1970), 247.

[20] As early as 1915 German Zeppelin airships had bombed English towns and cities; however, it was the Gotha raids that prompted the grand strategic reaction of formation of the Royal Air Force. For more details see Raymond Fredette, *The Sky of Fire: The First Battle of Britain 1917-1918 and the Birth of the Royal Air Force* (New York: Holt, Rinehart and Winston, 1996).

[21] Air power was attractive to the Clausewitzian trinity of the people, military commanders; and political leaders. The response to this realization was the formation of the Royal Air Force. Clausewitz, *On War*, 89.

nation.[22] Air power demonstrated that "God was no longer on the side of big battalions."[23] Such history rhymed with the emergence of cyber power. Cyber security has been elevated in the public consciousness, forcing governments to become focused and active regarding cyberspace issues.[24] CNN's depiction of electrical generators in cyber-induced death throes, [25] and the media-fuelled fallacy of cyber "fire storms," have resulted in cyber power being perceived as the new military equalizer that can bypass conventional forces to strike at the very fabric of one's nation.[26]

Control of the new air domain, whether for offensive or defensive purposes, became the cornerstone of air power theories. Douhet, the founding father of air power theory, declared that: "Command of the air is to have victory."[27] Control of cyberspace, evidenced in information dominance concepts, is a similar mantra of many cyber advocates. Douhet's words echo across the generations in the writings of Toffler: "The wars of the future will increasingly be prevented, won or lost based on information superiority and dominance."[28] Clarke is therefore fair in his assertion that a similar mentality now pervades American military thinking on the subject of the Fifth Battlespace: cyberspace is "a domain that the US must dominate."[29]

The military utility of the cyber domain, coupled with the widely held belief that national security is related to domination of cyberspace, marries the early development of air power to the contemporary development of cyber power. As the airplane developed and increased the utility of the air domain for military employ, so the military utility of

---

[22] Douhet, *The Command of the Air*, 10.

[23] "On dit que Dieu est toujours pour les gros bataillons." Translates: "It is said that God is always on the side of the big battalions." Voltaire in a letter to François-Louis-Henri Leriche, dated 6 February 1770. Quote drawn from John Carlin, 'A Farewell to Arms', *Wired*, May 1997. http://www.wired.com/wired/archive/5.05/netizen.html accessed 18 February 2011.

[24] Paul Cornish, *On Cyber Warfare*, (London: RUSI, 2010), 1.

[25] CNN's footage of Project Aurora, the staged demonstration of SCADA vulnerabilities, was first shown on 27 September 2007. http://www.cnn.com/2007/US/09/27/power.at.risk/index.html. The footage has been included in numerous documentaries including CBS's 60 Minutes episode entitled Cyber War: Sabotaging the System, 8 November 2009. http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml

[26] A fire storm, or fire sale, are terms drawn from fiction to describe a coordinated cyber attack on a nation's transportation, telecommunications, financial, and utilities infrastructure.

[27] Douhet, *The Command of the Air*, 25.

[28] Alvin Toffler, "Looking at the Future with Alvin Toffler," *USA Today* available at http://www.usatoday.com/news/opinion/columnists/toffler/toff05.htm accessed 5 January 2011.

[29] Clarke, *Cyber War*, 44.

the cyber domain, as information and networking technologies become ever more pervasive, will develop too. An examination of the technical nature of the air and cyber domains will further demonstrate that the kindred forces that steer their development paths go well beyond the merely superficial.

Science Fiction becomes Reality

Mankind's ability to overcome the bonds of the earth's gravity and conquer a new domain was not the product of Clausewitzian chance, or intellectual musings alone. The harnessing of technology was the means by which the Wright Brothers were able to avoid Lilienthal's catastrophic leap of faith.[30] Technology has been described as simply "physical artifacts or software." [31] The airplane is the embodiment of a technological artifact that has fundamentally changed the character of war. Technology enabled science fiction to become reality by unlocking the "secret of the flying machine" for military leaders to employ.[32] New strategic doors were opened: air power could now challenge the Leviathans of the ocean; or leapfrog armies to strike directly at an enemy's capital.[33]

But this paper has already contested that strategy must never be reactive, or subordinated to follow technology's lead. To do so carries with it the cognitive risk of technology being employed as a blackbox explanation governing air power's development along a pre-determined path. If such a technological deterministic position is accepted, any strategic analogy between air and cyber power will prove futile as it can be argued that cyber power's development path is pre-ordained.[34] Consequently, this paper contests that the airplane represented far more than a technological artifact.

---

[30] Otto Lilienthal produced extensive aerodynamic data between 1871 and his death in 1896. This work was published as *Der Vogelflug als Grundlage der Fliegekunst*, 1889. Translation: Birdflight as the Basis of Aviation. Lilienthal was killed during one of his aeronautical experiments when his monoplane glider stalled and crashed. For more details see Jakab, *Visions of a Flying Machine: The Wright Brothers and the Process of Invention*, 32-37.

[31] Thomas Hughes in Smith and Marx, *Does Technology Drive History?: The Dilemma of Technological Determinism* (Cambridge, MA: MIT Press, 1994), *102.*

[32] The term "secret of the flying machine" appeared in H.G. Wells' science fiction novel, *The War in the Air*, 1908.

[33] For example, see William 'Billy' Mitchell's passionate description of the sinking of the "unsinkable ship", the dreadnaught *Ostfiesland.* William Billy Mitchell*, Winged Defense,* (Tuscaloosa, AL: University of Alabama Press, 2009), 42-44 and 56-76.

[34] Technological determinism is the belief that changes in technology exert a greater influence on societies and their processes than any other factor. Rob Smith, *Does Technology Drive History*, 2.

Instead, it posits that the Wright Flyer heralded a fundamental change in the dynamic between the social, military and technical worlds. Man's ascent into the air domain is therefore better captured by Hughes' definition of technology as "a sociotechnical system that includes: institutions; values; interest groups, classes, political and economic forces."[35] Military leaders were forced to open the blackbox of air power and unravel the complexities of the relationship between technology and strategy.[36] Only then could development and employ of the airplane be actively marshaled towards strategic ends.[37]

At an analogically superficial level, air power and cyber power have obvious technological commonalities. The artifact that is the airplane represents the realization of a complex system of systems that must be harmoniously blended to gain access to the medium that is the air.[38] Cyber power's system of systems is composed of the now ubiquitous artifacts of the computer, software, and networking.[39] These elements of a computer network, when harnessed by man's imagination, have built and enabled access to the cyber domain: a domain that, like air before it, granted unprecedented reach, and an unparalleled speed of maneuver.[40] But a focus upon the technological artifacts of air and cyber power fails to recognize the new sociotechnical systems that air power and cyber power introduced. Cyber power's blackbox must be opened if strategic dystopia is to be avoided.[41]

---

[35] Hughes in Smith, *Does Technology Drive History?: The Dilemma of Technological Determinism*, *103.*

[36] Geoffrey Parker, *The Military Revolution: Military Innovation and the Rise of the West, 1500-1800* (Cambridge: Cambridge University Press, 1996), 157.

[37] John Law in Wiebe Bijker ed., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*,(Cambridge, MA: MIT Press, 1989), 114.

[38] Sir George Cayley originally conceptualized an airplane as consisting of three interdependent systems: a structure of sustaining surfaces that would provide lift; a means of propulsion to power the aircraft through the air; and a control system to balance the airplane in flight. J. Laurence Pritchard, *Sir George Cayley: The Inventor of the Aeroplane* (London: Parrish, 1961), 206.

[39] The System of Systems approach focuses on a system as a whole rather than discrete elements within a system. The concept was first described by Russell Ackoff, 'Towards a System of Systems Concept', *Management Science*, Vol 17, No 11, July 1971, 61.

[40] The term "maneuver at the speed of light" from Richard Clarke, 'War from Cyberspace,' *The National Interest*, Nov-Dec 2009.

[41] The term "strategic dystopia" is deliberately used to reflect significant concerns that have been raised at the highest levels of Defense in both the US and UK concerning the "lost institutional capacity for, and culture of strategy thought." See Robert Gates, "A Balanced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs*, January / February 2009; and Public Administration Select Committee, *Who Does UK National Strategy?*, 25 January 2011, 4.

Strategic Information Warfare, and air power before it, proffered the technologically-facilitated allure of an economic and precise means of attacking an adversary's center of gravity.[42] Air power's early development was not based upon a technological artifact, but rather the potential of technology that would not be truly realized until Operation DESERT STORM.[43] Cyber power's technical allure is not the capabilities demonstrated in Estonia, Georgia or Iran, but rather the potential it offers. But with potential comes risk, specifically the risk of over-expectation. Gray, when considering the early prophets of air power, stated that "often, the prophets are substantially correct, but rarely on the time scale they envisaged."[44] The emergent window between science fiction and reality, when a new technology is initially being applied to warfighting in a new domain, is when expectation and risk-management are most required. Libicki notes a similarly infectious optimism that is developing regarding cyber power, and counters that electrons must not be labeled the "ultimate precision weapon."[45] The allure of an unrealized potential of technology is what truly binds air power and cyber power's formative years. Like air power, the relationships between the technological agents that hide within the blackbox that is cyber power, will also be demonstrated to be fuzzy, non-linear, and prone to professional biases, and organizational interests.[46]

Fuzzy Boundaries

Lorenzetti's Allegory of Bad Government provides a perfect graphical depiction that a government's primary responsibility is to provide security for its people.[47] Insecurity, the product of Siena's crumbling walls, is portrayed as inducing rampant

---

http://www.publications.parliament.uk/pa/cm201011/cmselect/cmpubadm/713/713.pdf accessed 20 February 2011.

[42] Rattray, *Strategic Warfare in Cyberspace,* 81-84.

[43] Benjamin Lambeth, *The Transformation of American Air Power* (Ithaca, NY: Cornell University Press, 2000), 8.

[44] Colin Gray, *American Military Space Policy: Information Systems, Weapon Systems, and Arms Control* (Cambridge, MA: Abt Books, 1983), 1.

[45] Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 72.

[46] Stephen Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithica: Cornell University Press, 1994),18-22.

[47] Lorenzetti's Allegory of Good and Bad government is referred to by David Omand when considering security issues. The metaphor has been extended to the air and cyber domains for the purpose of this paper. David Omand, *Securing the State* (New York, NY: Columbia University Press, 2010), 2.

internal discord. This paper suggests that air power and cyber power are contemporary metaphors for Siena's walls: the challenge to a state's ability to maintain and secure its borders. Cyberspace has been described as a complex system of systems, and as Roodt notes, the boundaries of complex systems are inherently "fuzzy and permeable."[48] Indeed, the permeable boundaries of cyberspace have already been demonstrated in Chapter One in regard to the collateral damage that the Stuxnet worm wrought, well beyond the borders of the target system and state. But the analogical fuzzy boundaries that this analysis refers to are not the comparison of air and cyberspace as both being global commons that challenge the sovereign security of a state.[49] Instead, it is the consequence of this challenge that is focused upon: the internal discord that Siena's crumbling walls induced.

Air power is an appropriate lens for cyber power's development because the forces that influence their development are so closely related. The emergence of the Royal Air Force (RAF) and United States Air Force (USAF) were the products of security-induced internal discord: an imperfect commons of competing ownership claims. Inter-service rivalry and parochialism plagued air power's formative years in both nations.[50] Such debates were fuelled by the emergence of a visionary new form of warfare that threatened, as Smuts insensitively declared, that "older forms of military and naval operations may become secondary and subordinate."[51] At the superficial level, it can be contested that the cyber warrior's ascendancy to status as most favored child, lavished with the resource concomitant to such a position, mirrors the growth of air power. But such an explanation fails to grasp the wider analogical similarities at play within the blackbox of technology.

---

[48] J H S Roodt, R Oosthuizen, J C Jansen van Vuuren, *Boundary Management and Integration Framework for a Joint Cyber Defence Capability for Military Forces: Analysis and Synthesis from a Through-Life Capability Management Perspective,* Available at: http://researchspace.csir.co.za/dspace/bitstream/10204/4848/1/Van%20Vuuren1_2010.pdf accessed 10 February 2011.

[49] Denmark states that "the air commons offers an important model for how international norms and widely-accepted agreements can combine to sustain the openness of a commons." Abraham Denmark, "Managing the Global Commons," *The Washington Quarterly*, 33:3 165.

[50] For example see Arthur Gould Lee, *No Parachute: A Fighter Pilot in World War I; Letters Written in 1917 by A. S. G. Lee* (New York, NY: Harper & Row, 1970).

[51] H A Jones, *Official History of the War in the Air Appendices* (Clarendon, 1937), 8-14.

The transformational effects of cyber power go beyond artifacts and resources. For example, each of the US Services has stood up their own organizations to face the challenges of their own cyber dependency. The US Navy has established Tenth Fleet as its Cyber Command; the USAF created the Twenty-fourth Air Force; and the Second US Army has been reformed. None of these organizations come with the artifacts associated with each Service's primary battlespace.[52] Cyber power has demanded its own forces. Each has been developed, like air power's early years, in an inherently non-linear, and bottom-up fashion. Consequently, the Services have changed: cyber dependency, and the leveraging of cyber power, has demanded the evolution of a cadre of cyber experts. Cyber warriors play an increasing role in each of the Services, each performing functions more similar to their sibling-Service cyber experts than those associated with their own Service's primary domain. The transforming effects of technology have, as Collins argues, forced military officers to evolve.[53]

The implications of this evolution are exposed by application of Abbot's thesis that people in similar professions compete not just for resource, but more significantly, for jurisdiction: each group of professionals seek wider society's recognition of their exclusive right to govern practice.[54] Cyber power, like air power before it, represents a visionary form of warfare that each Service's body of "professionals at arms" will naturally aspire to govern: security-induced internal discord has been introduced between the branches of the Armed Forces. Fuzzy cognitive battle-lines pertaining to jurisdiction and control, not of resource, but of each Service's cyber operational interests and cyber-professionalism of arms, have been drawn. The resemblance to the battles fought between the land and naval domains, for jurisdiction over air power, is stark.

Whilst military boys will be boys, and the jurisdictional inter-service rivalries that dominated air power's early years have the potential to be revisited with the maturation of cyber power, it should also be noted that governance of security in cyberspace is not purely constrained to the military dimension. In his analysis of the threats and challenges

---

[52] "The fleet has no ships, and the air-force unit has neither aircraft nor missiles. Their weapons are ones and zeroes. Their battlefield is cyberspace." Clarke, *War from Cyberspace*.

[53] Brian J Collins, *Behind the Cyberspace Veil: The Hidden Evolution of the Air Force Officer Corps* (Westport, CT, Praeger, 2008), 5.

[54] Andrew Abbott, *The System of Professions: An Essay of the Division of Labour*, (Chicago, IL: University of Chicago Press, 1988), 3.

that cyber warfare presents, Cornish notes that the boundaries between the military and civilian facets of cyber power are blurred too.[55] What Cornish fails to note are the implications of this observation. Just as cyber professionals within the military are likely to mirror air power's development by competing for jurisdiction of the new domain, so this jurisdictional competition is also likely to permeate across the fuzzy boundary that exists between the military and civilian facets of cyber power. Indeed, inter-departmental discord regarding jurisdiction in the new domain has already been recognized: "turf rivalry between UK government departments has already hindered cyber policy."[56] This contemporary failure to satisfactorily address cyber space's fuzzy borders and jurisdictional issues is understandable when considered from the perspective of emerging professionalism. The following chapter's application of historical analogy to the evolution of air power's roles will provide a mechanism by which cyber power's fuzzy boundaries can be addressed, to allow this jurisdictional problem space to be broken into its constituent parts to facilitate more focused ownership.

As Thompson once warned: "History is the best teacher but its lessons are not on the surface."[57] The similarities between air power and cyber power, whilst obvious at the surface level, have also been demonstrated to go well beyond the merely superficial: herein will lie the lessons for cyber power's future. It has been shown that the forces that steered air power's development are also exerting their influence upon the evolution of cyber power. Air power and cyber power share a common recognition of the military utility of a new domain, coupled with a widely held belief that national security demands that the domain should be controlled. Whilst both domains represent the realization of science fiction, air power and cyber power's allure was not founded upon technical artifacts and "boy's toys", but rather the military potential that technology presented: Gray's caution that whilst prophets of air power and cyber power may be correct, a common bond of over-expectation, and risk, bind air power and cyber power together. Last, the fuzzy professional boundaries that induced jurisdictional battles in the

[55] Cornish, *On Cyber Warfare*, 10.
[56] Brian Loader, *Cyberspace Divide: Equality, Agency and Policy in the Information Society* (New York, NY: Routledge, 1998), 186.
[57] Kenneth Thompson, *Political Realism and the Crisis of World Politics* (Princeton, NJ: Princeton University Press ,1960), 36.

development of air power are evident in the military and cross-governmental facets of the cyber domain.

The Perils of Analogy

The development of air power has been demonstrated to have validity as a proxy for the void in cyber power's experience to date. In his consideration of how organizations and decision-makers learn, Jervis concurs that insights derived from analogy and previous events provide a useful shortcut to rationality. Rationality, that this paper has contested, may not be realizable as yet via inductive means. But Jervis also notes that analogy also serves to obscure aspects of the present case that are different from the past.[58] The perils of analogy are legion: perfect analogy; misperception; lazy analogy; and selection of the wrong analogy have all been referred to in this chapter. But a review of the other analogical dangers that must be avoided in forthcoming chapters is also pertinent at this stage.

Sheldon notes that "One of the major pitfalls of analogical reasoning is seeing what one wants to see, and ignoring inconvenient, awkward or unknowable aspects."[59] But analogical risks go beyond the conscious manipulation of marrying and discarding information. Analogy can have a significant impact at the unconscious level: this is the peril of insidious analogy.[60] Unintended analogical inference may be the by-product of lazy or emotive language. Indeed, the very title of this thesis, in conjuring images of the decimation of Dresden, may bias a reader's perception that the current path of cyber power is heading towards atrocity. This paper's inoculation against the subliminal side-effects of insidious bias will be to ensure that where non-neutral analogical language is used to emphasize a point, the risk will be exposed within the accompanying analysis, thus raising inference to a conscious and examinable level.

For air power's experience to be applied to cyber power, the peril of false analogy must also be avoided: the substance, as well as the logical inferences made in an

---

[58] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), 220.
[59] John Sheldon, *Reasoning by Strategic Analogy: Classic Strategic Thought and the Foundations of a Theory of Space Power*, 27.
[60] Fischer, *Historians' Fallacies*, 244.

argument, must be demonstrated to be sound.[61] For example, the development and employ of air power's actions in World Wars I and II represents the application of military force in total war: any lessons drawn from such extreme circumstances must be scrutinized and caveated regarding their applicability to limited cyber war. This is not to discard the potential relevance of lessons that may lie within air power's history; however, major contextual differences must be exposed to ensure that the validity of any lessons drawn is not undermined.

Insidious and false analogous share a common analytical solution: they can be exposed; and tested. This paper suggests that the most perilous analogical risk is that which cannot be exposed or tested. This is the cardinal sin of prediction by analogy. The danger in futurist analogies, as Fischer posits, is not that any conclusions reached may be erroneous. The analytical peril is simply that any conclusion is "utterly untestable," and thus logically inconclusive.[62] One can reason from cyber power's potential future, to an insight from air power's past; however, the process is not reversible. Consequently, this thesis will bound its analysis to ensure that air power's experience is only drawn upon to produce warning signs on the path of military cyber power development, rather than as a futurist development plan for cyber strategists to dogmatically follow.

Summary

This chapter has demonstrated that aspects of air power's history may rhyme with cyber power's future. Consequently, the guarded use of analogy, safely steered within the bounds of an analytical model, has been proposed so that air power's development may serve as a proxy for the relative void in cyber power's experience. This thesis has argued that the employ of Gray's operational, theoretical and organizational dimensions of strategy at the macro-level; blended with Khong's AE Framework at the micro-level, presents a means of drawing out lessons from air power's rich history. In turn, these lessons can be utilized to help build a short-term risk management strategy for the proactive development of cyber power.

Heeding Khong's warning that the most obvious analogies can also be the most superficial, care has been taken to determine if air power is an appropriate lens to apply

[61] For a detailed example of false analogy see Fischer, *Historians' Fallacies*, 252.
[62] Fischer, *Historians' Fallacies*, 257.

to cyber power's development. The factors that have influenced air and cyber power's development, whilst obvious at the surface level, have also been shown to go well beyond the merely superficial First, both are founded upon a recognition of the military utility of a new domain, coupled with a belief that national security demands that the emerging domain must be controlled. Second, whilst both domains represent the realization of science fiction, air power and cyber power's allure has not been founded solely upon technical artifacts, but also the military potential that technology presented. A significant point highlighted herein is that air power and cyber power may share a common bond of over-expectation. Third, the fuzzy professional boundaries that induced jurisdictional battles in the development of air power have been demonstrated to exist in the military and cross-governmental facets of the cyber domain.

Last, and by no means least, the limits and perils of analogy have been iterated to ensure that the lessons drawn from air power are appropriately utilized. It has been emphasized that air power's experience is best employed to derive warning signs on the path of military cyber power's development, rather than as a map for cyber power to unquestioningly follow. It is important to note that the psychological attraction of analogy is extremely strong for decision-makers, and has resulted in many bad ideas being preserved, and persevered with, well beyond their useful life. This thesis' satisficing employ of analogical reasoning, is thus deliberately incomplete so that any lessons drawn are not persevered with beyond the short-term. As Winton notes, a theory must have anticipatory value, yet analogical reasoning's fallacy of prediction reduces its utility in this area.[63] Inductive theoretical reasoning, coupled with analytical extrapolation of cyber's growing history, are likely to represent a more fruitful and complete means of forging a future guiding theory of cyber power.

[63] Winton, *An Imperfect Jewel: Military Theory and the Military Profession,* 7.

Chapter 3

THE STRATEGIC DIMENSION OF OPERATIONS – THE ROLES OF CYBER AND AIR POWER

Both Joint and interagency channels have highlighted the inadequacy of current terminology to describe our cyber operations capabilities and missions.

-- General Cartwright
Vice Chairman Joint Chiefs of Staff, 2010

This new arm had suddenly sprung into a field of war; and its characteristics, radically different from those of any other arm up to that time, were still undefined.[1]

-- Giulio Douhet, 1921

Therefore its name was called Babel, because there the Lord confused the language of all the earth.

-- Genesis, 11:9.[2]

A new arm has sprung into the field of war; an arm that is radically different from those of its sibling Services; an arm whose functions remain largely undefined. Similar sentiments, penned 90 years ago by Douhet, resonate with cyber strategists today. Indeed, General Cartwright has thrown down a "Douhetian" cognitive gauntlet, calling upon the military cyber community to address the Fifth Battlespace's ill-defined capability and mission set. But Kuhn's consideration of the structure of scientific revolutions suggests that this will be no simple task.

Kuhn noted that as a body of scientific knowledge and expertise develops, a co-incident emergence of an esoteric vocabulary is demanded to describe the new discipline and skills.[3] This refinement of concepts and terminology gradually diverges from the discipline's prototype paradigm: a paradigm which remains sacred to many of the discipline's founding fathers. Considerable resistance to change is the result. This thesis

[1] Douhet, *The Command of the Air*, 3.
[2] *English Standard Bible*, 2001.
[3] Thomas Kuhn, *The Structure of Scientific Revolutions*, (Chicago, IL: University of Chicago Press, 1996), 64-65.

suggests that the Fifth Battlespace today is a realm of such paradigmatic confusion. Emergent capabilities, in competing tribes of cyber professionals-at-arms, have spawned competing cyber terminologies. As these tribes become aggregated in the Joint and inter-agency space, competition for each tribe's lexicon to be adopted intensifies. A danger herein is that the founding fathers' prototype paradigm, whilst inadequate, may persevere beyond its useful life because it is the only common ground upon which the tribes can agree. This paper suggests that the persistence of the cyber terms Computer Network Attack (CNA); Computer Network Exploitation (CNE); and Computer Network Defense (CND) are relics of this prototype lexicon, all of which fail to characterize and define the cyber discipline's emerging capabilities and missions.[4]

Colin Gray defines strategy as the "use that is made of force and the threat of force for the ends of policy."[5] If the cyber discipline cannot characterize or define its capabilities and missions, how can the threat, or use, of force in the cyber domain be articulated to strategists? How can cyber power be wisely tailored to meet the ends of policy? If the beginning of wisdom is calling things by their right name, the answer to both of these questions is surely that "It cannot."[6] Unfortunately, the language of cyber space is a contemporary city of Babel: the consequence of Babel was not a bringing together of the tribes, but confusion leading to the dispersion of mankind across the earth. The lack of a common lexicon detailing cyber's roles is producing cognitive dispersion at a time when the efficient expansion and aggregation of cyber forces demands cohesion.

Turning first to the macro level of this paper's analogical analysis framework, Gray described the military operations dimension of strategy as the "threats and actions of organized bodies of warriors."[7] This is realm of "war proper." For the cyber strategist, it is the dimension that poses the fundamental question "How good are a state's cyber forces at fighting in cyberspace?" General Kehler iterated that "cyberspace is

---

[4] Paradoxically, whilst the Joint Terminology for Cyberspace Operations specifically recognizes the "inadequacy of current terminology to describe cyberspace operation capabilities and missions", Attachment 1 to the document then defines and perpetuates the terms Computer Network Attack, Computer Network Exploitation, and Computer Defense.

[5] Gray, *Modern Strategy*, 17.

6 Ancient Chinese Proverb, quoted by Paul McHugh, "Striving for Coherence: Psychiatry's Efforts Over Classification", *The Journal of American Medical Association*, no.293 (2005):2526-2528.

[7] Gray, *Modern Strategy*, 38.

about operations," but as Gray notes, the operational military dimension of strategy can often be neglected because it is thought to be so obvious:[8] scholarly focus on strategy is oft shifted too far from the battlespace.[9]

Applying Gray's observation to the micro-level of this paper's analysis, the nature of the problem facing cyber strategists, in terms of Khong's first step in the AE framework, is that the roles of cyber power in the battlespace, whilst appearing obvious, remain ill-defined. If cyber power's capabilities and roles cannot be defined, surely the operational fitness of a state's cyber forces cannot be critically assessed *en masse*. Clausewitz warned that strategy will always involve the "play of chance," but he also noted the import of probability in bounding and assessing man's "creative spirit."[10] To have no idea of the odds at which one is placing the strategic bet of employing military cyber power is to disregard Clausewitz's counsel, and subordinate strategic responsibility to the whims of man's creative spirit. Considered in terms of the second stage of Khong's AE framework, these are the operational risks that failure to address cyber power's muddled lexicon presents. Stage Three of Khong's framework therefore demands that a prescription be sought to fill this definitional void: an analysis of the emergence of air power's roles may provide a historical prism through which the military element of cyber power can be identified and broken into its constituent parts. These emerging cyber roles, in turn, may provide a means by which cyber's prototype lexicon can be discarded and more meaningful and coherent Fifth Battlespace roles identified for strategists to employ.

An Analysis of the Emergence of Air Power's Roles

The growth of air power, like cyber power today, will be demonstrated to be a non-linear, bottom-up process of emergence: an action-reaction cycle predominantly accelerated by the catalyst of hostilities in World Wars I and II.[11] Air power's military debut was borne of the recognition of the security granted by an airplane's speed and mobility, coupled with the unparalleled perspective inherent in this newfound freedom of

[8] Lionel Alford, "Cyber Warfare: The Threat to Weapon Systems," *WSTIAC Quarterly*, Vol 9, no.4, (Winter, 2009): 6.
[9] Gray, *Modern Strategy*, 38.
[10] Clausewitz, *On War*, 89.
[11] The "pressure of the World War, with its trial-and-error methods" dominated the development of air power. Douhet, *The Command of the Air*, 5.

maneuver. The result was that air power was perceived "first and chiefly" as an instrument of exploration and reconnaissance.[12] The keen-eyed observer or photographer, borne aloft by the airplane, was the realization of air power's inaugural military role as an Intelligence, Surveillance, and Reconnaissance (ISR) platform, serving both tactical and strategic level customers.[13] Air power had come to provide a uniquely powerful and focusable lens for Van Creveld's "directed telescope."[14]

Van Creveld's seminal work *Command in War* described the concept of a directed telescope: the requirement for a commander to be able to view any part of the enemy's forces, the terrain, or one's own army. This telescope could be trained from target to target, to meet a commander's specific momentary needs.[15] Air power not only provided a powerful lens for a commander's directed telescope, but also proffered a means by which commanders could transform this information into tactical and strategic advantage: air power's command, control and communication roles therefore soon followed on the heels of ISR: to deliver range-finding information to artillery units; or detail unit dispositions to guide the deployment of one's own infantry formations.[16]

But air power's non-kinetic roles of ISR and Command, were soon to be augmented with more direct military roles too. Appreciation of air power's "obvious advantage over surface means" was heralded by the airplane's long-anticipated role as a means to strike at the enemy on, and behind, his own lines.[17] The epitome of air power's evolutionary path as a bottom-up process of emergence occurred on 1 November 1911. On that historic day, Lieutenant Giulio Gavotti, a reconnaissance pilot attached to an Italian artillery unit, decided that air power's true calling lay beyond mere observation. Unbeknownst to his chain of command, Gavotti took to the air with four grenades, and upon his own volition launched an aerial attack upon the Turkish camp at Ain Zara.[18] Gavotti's unlicensed marriage of the airplane and the bomb, whilst not injuring anyone,

---

[12] Air power, in a reconnaissance and communication role was first employed by the Italians in Libya during the Italo-Turkish War of 1911-12. James Spaight, *Aircraft in War* (London: MacMillan, 1914), 8.
[13] Frederick Talbot, *Aëroplanes and Dirigibles of War* (London: Heinemann, 1915), 98.
[14] Van Creveld, *Command in War*, 147.
[15] Van Creveld, *Command in War*, 75.
[16] Talbot, *Aëroplanes and Dirigibles of War*, 100.
[17] Douhet, *The Command of the Air,* 3.
[18] Gerard De Groot, *The Bomb: A Life* (Cambridge, MA: Harvard, 2005), 2.

was reported as having "terrorized in the Turks."[19] Irrespective of the fact that air power's inaugural bombing raid was widely condemned as a gross defilement of the gentlemanly air of war, the gravitational attraction of the potential of aerial bombardment proved simply irresistible for military strategists. By June 1917, "war from the air" was no longer constrained to the realm of close air support and the near-battlefield: interdiction had become a commonly employed role for air power; and with the Gotha raids on London, air power's deep strike role was actualized.[20] A simplistic lexicon, containing only high-level terms such as air attack could not sufficiently define the breadth air power's roles. Instead, it was recognized that air power's offensive roles required a greater level of granularity in their means of categorization if they were to be understood and thereby more effectively employed. Consequently, a more expansive lexicon emerged.

Attack from the air came to be broken down into four broad categories: deep attack; counter-land operations; counter-sea operations and information operations.[21] Deep attack described the employment of air power to disrupt or destroy enemy centers of gravity and other important target sets including: an adversary's leadership; command systems; war production resources; fielded forces including reserves; and any other key supporting infrastructure. Air power's counter-land missions were designed to maximize the synergy between air and land forces to gain and maintain a desired degree of control of the land domain by targeting fielded enemy ground forces and the infrastructure directly supporting them. Three specific counter-land mission sets were to emerge: air interdiction;[22] close air support; and air operations for psychological effect.[23]

The third category of attack from the air, that of offensive counter-sea operations, rapidly evolved beyond Mitchell's ostensibly defensive demonstrations of air power's

---

[19] Lee Kennet, *A History of Strategic Bombing* (New York, NY: Scribner, 1982), 13.
[20] H G Wells, *The War in the Air* (London, Penguin, 1907)
[21] Air Publication (AP) 3000 Edition 4, 2009, 54. These air power functions are also iterated in US doctrine. See US Air Force Doctrine Document (AFDD) 1, 17 November 2003, 40.
[22] For example, Italian air doctrine detailed air interdiction concepts against road, rail and canal supply routes as early as 1915.
[23] The psychological impact of air power to, for example, "terrorize the Turks" is regarded as an effective non-kinetic means of exerting influence and attacking that most intangible, yet important military target: an adversary's will.

ability to find and attack maritime threats to the US coastline.[24] Indeed, a triumvirate of maritime-oriented missions emerged: the maturation of anti-surface warfare witnessed the RAF destroy 51 percent of Axis shipping; anti-submarine warfare came of age with Allied aircraft accounting for the sinking of over 47 percent of German U-boats in World War II; [25] and aerial mining became a new means of asserting control over Mahan's vital sea lines of communications.[26] All missions would be added to the modern air power lexicon.

Last, just as air power's attack roles against its sibling land and sea domains were captured, so air power's capability to attack the electromagnetic spectrum and cognitive realms were also identified under the predominantly non-kinetic umbrella mission set of information operations. Air power, harnessed to deny an enemy free use of the electromagnetic spectrum was embodied in its electronic warfare mission; and operations designed to affect behavior, communicate intent, or project accurate information to an adversary, fell into the role of influence operations. In sum, the plethora of offensive air power roles had soon been drawn together in a detailed lexicon that utilized a taxonomy based upon the specific target categories that air power could be employed against. It should not be surprising therefore that advocates, including Trenchard, espoused that air power was best employed as "a relentless and incessant offensive" tool. [27] But with the certainty of Newtonian physics, air power's offensive actions prompted an equal and opposite defensive reaction. [28]

As early as 1915, defensive developments in the form of pursuit aviation and ground-based anti-aircraft guns would result in the air domain, like land and sea before it, becoming a contested military medium.[29] The nation that attained control of the air also

---

[24] Tami Davis Biddle, *Rhetoric and Reality in Air Warfare*, 129.
[25] Stephen Roskill, *The War at Sea, 1939-1945, Vol 3* (London: HMSO, 1961), 457-472.
[26] Alfred Thayer Mahan, *The Influence of Sea Power on History (1660-1783)* (Annapolis, MA, Naval Institute Press, 1991).
[27] Sir Hugh Trenchard, A Memoranda on Air Tactics and Strategy, AIR/1/52216/12/5 reprinted in Maurice Baring, *R.F.C H.Q. 1914-1918* (London: Bell, 1920).
[28] Newton's Third Law is also referred to as the Action-Reaction Law. The law states that the mutual forces of action and reaction between two bodies are equal, opposite and collinear. Consequently, whenever a body exerts a force F on a second body, the second body exerts an equal and opposite force, −F, on the first body.
[29] James Olsen ed., *A History of Air Warfare* (Washington, D.C.: Potomac Books, 2010), 10.

attained the potential to master the earth.[30] Consequently, counter-air missions composed of both offensive and defensive facets came to be included in air power's ever-growing taxonomy. Two main categories of missions were identified: offensive counter-air; and defensive counter-air. Regarding the former, offensive counter-air missions evolved to encapsulate air operations that focused upon the destruction, disruption or degradation of an adversary's air power, either by destroying aircraft on the ground, or as close to their home airfield as possible. Offensive counter-air missions therefore included roles such as surface attack missions; air-to-air combat; suppression of enemy air defenses, and electronic warfare. In contrast, defensive counter-air missions were regarded as air defense in its purist form, consisting of both active and passive elements. Active air defense evolved well beyond the concept of pursuit aviation and encapsulated any air operation aimed at detecting, identifying, intercepting and destroying enemy air forces. Passive air defense represented an unconscious acceptance of Britain's Lord President of the Council, Stanley Baldwin's infamous statement that "the bomber will always get through" and included all measures taken to minimize the effectiveness of attack such as concealment, deception, dispersion, and today's stealth technologies.[31]

Bookending the air power roles that emerged from the hostilities of World Wars I and II would be another non-kinetic function. If the "eyes of air power" in the form of ISR were the first role in the military air power portfolio, it would be "the long arm of air power" in the form of air transport that would be the final addition.[32] At the strategic level, the treacherous airlift corridor established across the wonderfully understated Himalayas Hump would reach out air power's long arm: an airlift effort that would prove to be essential to the Allies' sustainment of their war effort in China. At the tactical level, aerial resupply to the battlefields of Burma facilitated what General Slim described as "the greatest defeat in the history of the Japanese Army."[33] The role of air mobility had come of age.

---

[30] Mitchell, *Winged Defense*, 26.
[31] Stanley Baldwin, *House of Commons Debates*, 10 November 1932, Vol 270, Col 632.
[32] The term "long arm of air power" is drawn from Probert., Henry Probert, *The Forgotten Air Force: The Royal Air Force in the War Against Japan, 1941-1945* (London, Brassey's, 1995), 194.
[33] Probert, *The Forgotten Air Force: The Royal Air Force in the War Against Japan, 1941-1945*, 192.

The historical relevance of these four fundamental air power roles remains valid in the contemporary context. Indeed, ISR, target-categorized air attack, control of the air, and air mobility all underpin UK and US air power doctrine and it is from these four fundamental roles that all of the aforementioned capabilities and missions flow.[34] Moreover, it is from these four roles that a coherent and "demystified" air power language and lexicon has formed.[35] Air power's lexicon may therefore serve as a Khongian surrogate for cyber power's paucity of military operations terminology.

Former Secretary of the Air Force Michael Wynne wrote, "All aspects of air war will have some equivalent role in cyber war."[36] Such an assertion, without supporting evidence is guilty of Howard's charge of analogy being employed as a "lazy substitute for analytical thought."[37] This paper's framework therefore demands that these four air power roles be scrutinized for their applicability to describe cyber power.

A Suitable Lexicon for Cyber Power?

Considering first the role of ISR, Sun Tzu famously instructed that one should "know the enemy."[38] This mantra remains the very essence of ISR, whose activities can be summarized as those that contribute to the creation of the intelligence preparation of the battlespace, and provide commanders with a detailed knowledge and understanding of the enemy.[39] From its inception, air power enhanced the commander's means of "knowing his enemy" in the air, land and sea battlespaces. Can the same be said of cyber power? At first glance, the longevity of the term CNE would suggest that this is the case. But CNE is defined as those intelligence collection capabilities conducted through the use of computer networks to purely gather data about an adversary's information systems or network infrastructure.[40] To that end, CNE is focused purely upon the Fifth Battlespace and bounded to activities such as the scanning and enumeration of an adversary's

---

[34] AP 3000, 37.
[35] AP 3000, 9.
[36] M.W. Wynne, "Flying and Fighting in Cyberspace," *Air and Space Power Journal,* Vol. 21, no. 1, (Spring 2007). http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/spr07.pdf (accessed 18 March 2011).
[37] Michael Howard, *The Causes of Wars and Other Essays* (London: Temple Smith, 1983), 132.
[38] Sun Tzu, *The Illustrated Art of War* (Boston: Random House, 1998), 125.
[39] See Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, 7 October 2004.
[40] James Cartwright, Vice Chairman of the Joint Chiefs of Staff, *Joint Terminology for Cyberspace Operations*, November 2010.

networks for security vulnerabilities. This thesis concurs with Libicki's most emphatic assertion that intelligence of a target is the *sine qua non* of conquest in cyberspace: CNE is essential to enable plans to be built to exploit or attack an enemy's networks. But it also contests that such a bounded definition for CNE renders it but one sub-category of cyber power's wider, more fundamental, ISR role.[41] Moreover, this paper asserts that the value of the term CNE is questionable because its meaning has become overly diffuse. For example, the Joint Terminology for Cyberspace Operations employs the term Joint Intelligence Preparation of the Operational Environment (JIPOE), rather than CNE, for all cyberspace operations that identify or map network topologies and adversary capabilities for any specific kinetic operation.[42] A more coherent titular alternative to CNE within the cyber lexicon is therefore suggested: Joint Intelligence Preparation of the Cyber Environment (JIPCE). A further facet of this cyber ISR role is exposed by returning to Sun Tzu. *The Art of War* posits that knowing the enemy is but one ingredient to success in battle: knowing oneself is of equal import.[43] JIPCE therefore must be composed of both friendly and enemy-oriented facets if it is to be effective: the twin roles of JIPCE (Enemy) and JIPCE (Friendly) are therefore demanded.

This paper's definition of cyber power is grounded in the ability to "use cyberspace to create advantages and influence events in its sibling operating environments."[44] Cyber power's ISR role, like air power before it, must therefore not be constrained to its own domain: cyber-facilitated ISR must also focus the commander's directed telescope upon its sibling domains. The simplest demonstration of the broader applicability of cyber's ISR role is the utilization of Internet search engines. As WikiLeaks has most ably exposed, organizational security procedures are rarely infallible and cyber space's porous borders allow pan-domain, operationally critical information to leak into the public realm.[45] Search engines, as well as more sensitive means, therefore

---

[41] Libicki, *Conquest in Cyberspace*, 90.

[42] *Joint Terminology for Cyberspace Operations*, 11.

[43] Sun Tzu, *The Illustrated Art of War*, 125.

[44]This paper's definition of cyber power is not unique in this context. For example see Dan Kuehl, *From Cyberspace to Cyberpower: Defining the Problem* (Washington D.C., NDU Press, 2009), 16.

[45] This paper uses the term wikileaks.org to encompass the original web-site and all of the many proxy versions. WikiLeaks' mission statement is: "WikiLeaks is a non-profit media organization dedicated to bringing important news and information to the public. We provide an innovative, secure and anonymous

represent methods by which military cyber ISR can be employed to advance a commander's holistic understanding of an enemy. [46] Having thus confirmed that an ISR role exists in any future cyber taxonomy, this paper will now turn its analysis upon the role of cyber attack.

Studies evidencing that the cyber domain can be employed for offensive military purposes abound.[47] Indeed, a constant stream of strategic analyses considering warfare in the Fifth Battlespace have been produced since Molander's *Strategic Information Warfare: A New Face of War*, and Rattray's *Strategic Warfare in Cyberspace* provided the foundations for this ever-burgeoning body of academic literature.[48] Theory has also, to a limited extent, been augmented by experience with the cyber-skirmishes of Estonia, Georgia, and most recently, Iran. Moreover, the cyber lexicon acknowledges that attack options exist by the continued inclusion of the term CNA.[49] Consequently, if literature, experience and doctrine all demonstrate that cyber attack is a very real threat, and a militarily useful tool, is any further advantage to be gained in analyzing the role of cyber attack here? If this analysis is to add granularity to the definitions of operational cyberspace, the taxonomy of air power must be demonstrated to be applicable for cyber power. Cyber attack is thus not viewed as a *sui generis* form of warfare, but rather that specific facets of air attack, if shown to marry with cyber attack, can help define the potential attack roles that cyber will play.

This thesis identified that the main facets of air attack are: deep attack; counter-land operations; counter-sea operations and information operations. Considering first the role of deep attack, Owens *et al* noted that cyber attack could be used to disrupt or

---

way for independent sources around the world to leak information to our journalists." See http://213.251.145.96/ (accessed 20 January 2011).

[46] For example, Signals Intelligence represents a more clandestine means of pan-domain ISR being conducted via cyber means.

[47] For example, see William Owens et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009).

[48] Roger C Molander, Andrew Riddile, and Peter Wilson, *Strategic Information Warfare: A New Face of War* (Washington D.C.: RAND, 1996).

[49] CNA is defined as "a category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate or destroy information resident in the target system or computer networks. The ultimate effect is not necessarily on the targeted system itself." *Joint Terminology for Cyberspace Operations*, 3.

destroy an adversary's C2 systems, air defenses, a nation's war-making infrastructure and industrial base, fielded forces, and war-fighting infrastructure.[50] This potential target list closely resembles Warden's five-ring framework that details how air power can be employed to strike systematically at an adversary's center(s) of gravity and other key infrastructure.[51] Owens' argument is supported by Rattray's demonstration that cyber power can be employed against such an expansive target set.[52] The Stuxnet worm has also put practical experience upon these theoretical bones to provide a glimpse of cyber's deep strike capabilities in the form of exploiting SCADA vulnerabilities from afar. Cyber power is therefore most definitely following in air power's footsteps of pursuing a deep strike role. The allure of a new means to strike at the enemy behind his own lines, coupled with the security granted of cyberspace's ability to operate from unparalleled range, may prove as irresistible as Gavotti's marriage of the airplane and the bomb. This temptation will be considered in more detail in the next chapter.

The potential import of a counter-land role for cyber power is well demonstrated by consideration of contemporary land combat formations. The US's 4th Infantry Division, often referred to as the "Digital Division," exemplifies the level of interconnectedness and cyber-dependency that has come to characterize the UK and US's NCW-era ground forces.[53] The Digital Division's "combat lethality, survivability and speed are achieved through information age technologies and logistic efficiencies."[54] Alberts and Hayes' *Power to the Edge* principles have been adopted, with cyberspace facilitating a revolution in command processes, typified by applications such as Blue Force Tracking and pull-oriented logistics chain methodologies.[55] Assault upon C2 systems and their associated data-links; network-enabled weapon systems; and their

[50] Owens, *Cyberattack Capabilities*, 21.
[51] Warden's rings are: leaderships; organic essentials; infrastructure; population; and field military. See John Warden, *Employing Air Power in the Twenty-first Century* (Montgomery, AL, Air University Press, 1992), 62-68.
[52] Rattray, *Strategic Warfare in Cyberspace*, 91-93 and 197-199.
[53] Ewen MacAskill and Stuart Miller, "America's Digital Division, - the Biggest Advance in Warfare since the Tank," *The Guardian,* 7 April 2003, 7.
[54] " 4th Infantry Division."http://www.globalsecurity.org/military/agency/army/4id.htm (accessed 11 Match 2011).
[55] Alberts, *Power to the Edge*, 6 and 88.

supporting logistics chain, all represent means by which cyber power can potentially be employed synergistically with sister domain capabilities to degrade an enemy's land forces.

Air power's counter-sea role has been represented in this paper by the destruction of Axis surface and sub-surface fleets. Cyber-power's potential counter-sea role, whilst not as dramatic as the depiction of air power's destructive capacity, could prove to be no less effective or efficient. To expand, on 21 September 1997, the cruiser USS Yorktown was on maneuvers as part of the Smart Ship Program off of the coast of Virginia. The attack the Yorktown experienced was nothing more dramatic than one of the ship's crew entering a zero into a database field. The effect was the complete failure of the ship's propulsion system.[56] The image of the USS Yorktown, stricken in the waters of the Virginia littoral, paints a striking contemporary equivalent of the *Ostfriesland.*[57] A modern warship, dead in the water due to the most simple of programming flaws, represents just one means of how a savvy cyber operator could seek to attack maritime forces without the need to fire a single missile or drop a single bomb.[58]

The potential of counter-air cyber attack, at the most obvious level, conjures sensationalist images in the mind's eye's of a manned aircraft's fly-by-wire flight controls being hacked into; or an armed UAV's remote control system being hijacked.[59] But less dramatic, yet arguably more plausible cyber attacks against our nations' air forces have already taken place. For example, the widely reported theft of data regarding the Joint Strike Fighter does not simply represent a means by which an adversary's own platform development cycle can be accelerated.[60] Early access to terabytes of design data may also provide a means by which an aircraft could be analyzed for weakness: a version

---

[56] "Sunk by Windows NT," *Wired*, dated 24 July 1998.

[57] The ex-German dreadnaught Ostrfriesland was sunk by aerial bombardment on 21 July 1921 as part of Billy Mitchell's trials to demonstrate the "domination of seacraft by aircraft". For a full account see Mitchell, *Winged Defense*, 67-73.

[58] A divide-by-zero error was allowed by the flaw in the database design. For more details see Gregory Slabodkin, "Navy CIO Orders an Investigation of Yorktown Systems Failure," www.cs.virginia edu/~survive/NEWS/news003.txt, August 31, 1999.

[59] For example, Robert Clarke, *Cyber War*, 204-205.

[60] For example see "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, 21 April 2009. http://online.wsj.com/article/SB124027491029837401.html . It has also been suggested that the J-20 design may have been based on cyber-espionage. For example see Thomas McInerney, "'Stealth' Chinese Fighter Jet Photos No Accident." *Fox News*, 6 January 2011.

of what Bunker describes as "cyber stripping" of stealthy and defensive design.[61] It was, after all, General Dodana's analysis of stolen data that led to the realization of the Death Star's weakness. Only then could Luke Skywalker know to aim his photon torpedo into the single thermal exhaust port that would cause the devastating chain reaction.[62]

The last facet of air power's attack roles to be considered is that of Information Operations and whether cyber power has a role to play in targeting the cognitive and electromagnetic realms of an adversary's decision making process. Information Operations' doctrine defines the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive."[63] This paper's definition of cyberspace emphasizes that it is a man-made physical domain, constructed for the purposes of informational exchange, to support the ends of creating effects. As Murphy points out, the rapid evolution of the information environment has caused the "information weapon" to rise in importance.[64] The growth of cyber power has been the driving force behind this evolution and as Kuehl notes, cyberspace now constitutes a key element of the informationalized battlespace through which "strategic influence is conducted."[65] Consequently, cyber power has a core and ever-expanding role to play in future Information Operations campaigns.

Air power's offensive roles have all been demonstrated to have an equivalent in the cyber domain, and a range of terms has been identified whose descriptive potential far exceeds the current poor fare of CNA. But the allure of the offense will not lead this thesis' analysis astray into the Douhetian folly of ignoring one's defense.[66] Rather, validation of cyber power's offensive roles demands an examination of the defensive facets of cyber power and the third major role of cyber power: control of cyberspace.

---

[61] Robert Bunker, *Five-Dimensional (Cyber) Warfighting: Can the Army After Next Be Defeated Through Complex Concepts and Technologies?* March 1998, 24.
[62] Note: reference to the science fiction classic, Star Wars Episode IV: a New Hope.
[63] Joint Publication (JP) 3-13, *Information Operations*, 10.
[64] Dennis M. Murphy, "Talking the Talk: Why Warfighters Don't Understand Information Operations," *IO Journal*, Vol 1, no. 1, (April 2009): 18-19.
[65] Keuhl, *From Cyberspace to Cyberpower*, 29.
[66] Douhet, *The Command of the Air*, 109.

Whilst the potential role of control of cyberspace is absent from the Joint Cyberspace Lexicon, the term cyberspace superiority is defined: "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force…without prohibitive interference by the opposing force." [67] Moreover, the definition's striking similarity to that of air superiority is also iterated.[68] But as air power doctrine states, air superiority is simply a degree of control over a specified portion of the air domain.[69] This thesis therefore argues that one cannot have cyber superiority without an equivalent umbrella role: control of cyberspace.

Control of the air, as has been described earlier in this chapter, is composed of both offensive and defensive counter-air operations.[70] Control of cyberspace, in demanding a degree of freedom of action for oneself, whilst inhibiting an adversary's freedom of maneuver, is also likely to have offensive and defensive facets. This thesis therefore posits that control of cyberspace is composed of offensive counter-cyber operations and defensive counter-cyber operations.

Offensive counter-cyber activities, founded upon the principle of destroying the enemy's offensive capabilities before they can be employed to inhibit one's own freedom of maneuver, include two distinct sub-roles that have parallels with air power: attack against an enemy's cyberspace forces and capabilities; and suppression of enemy cyber defenses. [71] Cyberspace, composed as it is of physical, electromagnetic, and informational elements, can potentially accommodate attacks via any of these vectors. It is therefore important to note that offensive counter-cyber effects are not constrained to actions conducted purely within the cyber domain. Kinetic attack could be launched against important server farms and physical network infrastructure; electronic warfare and directed energy weapons could be employed against the wireless medium or

[67] *Joint Terminology for Cyberspace Operations*, 8.
[68] Joint Publication 1-02 defines air superiority as: "That degree of dominance in the air battle of one force over another that permits the conduct of operations by the former, and its related land, sea, and air forces in a given time and place without prohibitive interference by the opposing force."
[69] JP 3-30, ix.
[70] AP 3000 4th Ed, 39.
[71] Note: Attack against an opponents forces may take place before, during, or after use of their own weapons systems.

processors; and the more familiar military cyber capabilities such as malware and botnets are also likely to endure.

Just as offensive counter-cyber has been demonstrated to be multifaceted, so too are defensive counter-cyber operations. This paper suggests that cyber defense, like air defense, consists of both active and passive elements. Active cyber defense encapsulates all cyber operations aimed at detecting, identifying, intercepting and destroying enemy forces attacking via the cyber domain: anti-malware detection; firewalls; intrusion detection systems; and incident response teams all fall within this role. Passive cyber defense, to paraphrase Baldwin, acknowledges that "the hacker always finds a way through." Thus passive cyber defense includes all measures taken to minimize the effectiveness of attack such as: concealment and redirection; forms of military deception including honey-pots; and designed-in resilience via robust back-ups, patching, tight privilege control processes, and dispersion.[72] As will be shown in the next chapter, the import of passive defense to the cyber warrior cannot be over-emphasized because as Libicki notes, there is no such thing as forced entry in cyberspace: all elements of a computer network are ultimately under the control of the owner.[73] In the cyber domain, if one's adversary always finds a way through, it is only because we have created the path for the belligerent to exploit.

An analogical analysis of the concept of control of the air has demonstrated that it has applicability in the Fifth Battlespace. Moreover, the breadth of sub-ordinate control of cyberspace activities demonstrates the inadequacy of the current cyber lexicon. CND, like the terms CNE and CNA, has once again been exposed as inferior in comparison to adaptation of the lexicon of air power.

The final role in military air power's portfolio to be considered is that of mobility. Air mobility extends the reach of military forces, and facilitates flexible, rapid, and timely options to apply strategic influence in kinetic and non-kinetic crises.[74] In short, air mobility grants the UK and US the ability to deliver and sustain expeditionary forces,

---

[72] The term hacker used in the sense of a deliberate military attack, rather than a criminal act perpetrated by a private individual.

[73] Libicki, *Conquest in Cyberspace*, 31-37.

[74] The Himalaya Hump has already been described in this paper and serves as an excellent example of air mobility extending support to kinetic operations. In contrast, the Berlin Airlift provides an example of air mobility's facilitation of strategic influence via non-kinetic means.

logistics support, and infrastructure into theatre with the minimum of delay.[75] Trias and Bell, in their analysis of cyber power, contest that air mobility has an equivalent role within the cyber domain: cyberlift.[76] Their argument is founded upon the premise that cyber mobility, by delivering a payload of information to theatre, represents an increase in the operating range of military forces. "Getting the right information, to the right person, at the right time," has long been the strap-line of the NEC and NCW communities; however, this paper contests that employing the long-arm of the Fifth Domain to transfer software patches, email, and imagery, whilst important, cannot mirror air power's ability to sustain a kinetic fight, or feed a starving populace. Packets of information are not the cyber equivalent of pallets of ammunition and paratroops, so essential to sustain Slim's battlefields of Burma. Cyber power, in terms of the informationalized battlespace, provides the means by which "strategic influence is conducted" from afar, but it does not have the ability to deliver and sustain expeditionary forces, logistics support and infrastructure into theatre.[77] This paper therefore concludes that Wynne is wrong: not all aspects of air war will have an equivalent role in cyber war.[78] Air power's role of mobility does not have a place in the cyber lexicon.

Conclusion

This chapter has picked up the cognitive gauntlet thrown down by Douhet and Cartwright. The prism of air power has been applied to cyber power and a spectrum of cyber roles, more glorious in color and richness than the contemporary equivalents of CNA, CNE and CND, have been exposed. A coherent and demystified cyber lexicon has been proposed. A lexicon that, at the top level, identifies a Clausewitzian triumvirate of roles for cyber power: ISR; cyber attack; and control of cyberspace. Within each of these roles, subordinate cyber missions have been identified. Within the ISR role, as well as providing support to cyber's sibling domains, the missions of JIPCE (Friendly) and JIPCE (Enemy) have been proposed. In terms of cyber attack, the roles of deep attack;

---

[75] AFDD 2-1, Air Warfare, 17, http://www.dtic.mil/doctrine/jel/service_pubs/afd2_1.pdf (accessed 24 March 2011).

[76] For full details see Eric Trias and Bryan Bell, *"Cyber This, Cyber That…So What?," Air & Space Power Journal*, Vol. 24, no. 1,(Spring 2010).

[77] Keuhl, *From Cyberspace to Cyberpower*, 29.

[78] Wynne, M.W., "Flying and Fighting in Cyberspace," *Air and Space Power Journal,* Vol. 21, No. 1, Spring 2007, http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/spr07.pdf (accessed 18 March 2011).

counter-land; counter-sea; and information operations have all been demonstrated to have applicability. Last, the core function of control of cyberspace was considered, and a case presented to support the need for offensive and defensive counter-cyber operations, the latter being composed of both active and passive functions.

But an applicable lexicon is only half of the battle. For the consequences of Babel to be avoided, the Kuhnian challenges of adoption must still be overcome. This framework to define cyber power's roles does not stand without competition. For example, Alford proposes a more chronological and action-driven taxonomy, deconstructing cyber attack into the subordinate functions of infiltration, assault, manipulation and raid.[79] But the failing of taxonomies such as Alford's, in comparison to this thesis' utilization of air power's lexicon, is that it does not bound specific target sets and capabilities. By not specifying target-sets, you are not specifying the target capability one wishes to disarm the enemy of.[80] Furthermore, in taxonomies like Alford's, or the extant terms CNA, CND and CNE, military cyberspace's fuzzy borders remain cognitively porous. Cyber attack does not exclude terrorists, criminals, perpetrators of commercial and state espionage, or amateur hackers. In contrast, this paper's taxonomy serves to bound the military problem space. By defining discrete military roles that cyber forces must satisfy, this paper reiterates Ryan and Ryan's conclusion that cyber warfare is "first and foremost, warfare."[81] Terrorism, crime, and espionage, whilst acknowledged as being important national security issues, are deliberately excluded to ensure that the pressing challenge of forging coherent military forces is not diverted.

Now that this paper is armed with clearly articulated roles for cyber power, their relative import will be assessed. This will be the subject of next chapter's analysis of competing cyber paradigms. But it is important to highlight that the perils of analogy remain present in this analysis. For example, the title deep attack has been employed herein, rather the terms strategic or independent cyber attack used by Molander and

---

[79] Alford's taxonomy suggested the following: actions following cyber infiltration can affect organizations via the transfer, destruction, and altering of records (cyber raid); software within systems can be manipulated and the systems controlled by that software can be damaged or controlled (cyber manipulation); software itself can be copied, damaged, or rewritten (cyber assault).

[80] Clausewitz noted that to compel an enemy to one's will an opponent must be disarmed.

[81] Daniel Ryan and Julie Ryan, *Protecting the NII against Infowar*, in Information Warfare (Thunder's Mouth Press, 1996).

Rattray. As noted in Chapter 2, unintended analogical inference can be the by-product of lazy or emotive language. This paper contests that there are insidious biases inherent in these latter terms that a cyber lexicon must avoid: strategic can be misinterpreted as important; and independent can bias organizational structures and investment focus. The ensuing analysis will consider future cyber developmental choices, exposed and hopefully immunized to this bias.

A final disadvantage inherent in this thesis' use of analogy is that mapping air power's extant taxonomy to cyber does not expose where cyber power may have roles that simply do not exist in air power. This analogical framework therefore only serves as a springboard for the development of cyber power's taxonomy and future inductive study is demanded.

Chapter 4

THE STRATEGIC DIMENSION OF THEORY AND DOCTRINE - THE PERILS OF COMPETING PARADIGMS

Resign oneself to submit to enemy attacks in order to use all possible means for launching the greatest offensives against the enemy.

-- Giulio Douhet,
The Command of the Air

A mere bald-headed unreasoning offensive, simply for the sake of the offensive, is unlikely to be any more effective today than it was in 1914.

-- J. C. Slessor,
Air Power and Armies

There is no silver bullet against information warfare attacks.

-- Dorothy Denning,
Information Warfare and Security

Armed with a framework for a revised cyber lexicon, this thesis has completed the first step demanded of a theory of cyber warfare: a taxonomy of foundational terms and roles, drawn from the evolution of air power, has been introduced and defined.[1] But as Winton notes, for a theory to have utility, it must also connect these foundational elements so that they can be treated as a comprehensive whole. Unfortunately, "the compelling need for a comprehensive, robust and articulate cyberpower theory," to describe the relationship between these foundational elements remains unsated.[2]

The strategic peril inherent in this cognitive void cannot be understated. As Cornish asserts, guiding strategy and doctrine is "essential to the creation and development of a national cyber warfare capability."[3] Gray's dimensions of strategy provide academic credence to this statement when highlighting that it is theory, as the body of ideas and thinking, that drives strategic behavior and provides guidance to military forces.[4] Theory is the foundation upon which all preparation for war is built. If operational cyber capabilities are to be developed and employed as a comprehensive

---

[1] Winton, *An Imperfect Jewel: Military Theory and the Military Profession*.
[2] Quote drawn from the Terms of Reference for study of "A Theory of Cyberpower", March 2006. See Starr, *Toward a Preliminary Theory of Cyberpower,* 46.
[3] Cornish, *On Cyber Warfare*, 16.
[4] Gray, *Modern Strategy*, 35.

whole, rather than as emergent individual elements, a surrogate theory for military cyberpower is therefore demanded. Herein lies the Khongian risk that the lack of a unifying theory of military cyber power presents. The focus of this paper's macro-level analysis will therefore now be turned upon air power's guiding theories to assess their utility to help safely steer the evolution of cyber power through its current *interregnum,* and until its own inductive theory reaches a level of maturity whereupon it is fit to assume cognitive sovereignty.

But a caveat must also be made at this point. Theory is vitally important, but as has already been noted, it is an imperfect jewel and can never be more than a cognitive guide. As Clausewitz rightly cautioned: "Theory cannot equip the mind with formulas for solving problems, nor can it mark the narrow path on which the sole solution is supposed to lie by planting a hedge of principles on either side. But it can give the mind insight into the great mass of phenomena and of the relationships, then leave it free to rise into the higher realms of action."[5] The following analysis' consideration of air power's guiding theories will therefore not seek to reach a digital conclusion that one air power theory fits cyber power's needs best. Instead, contrasting air power theories will be considered as potential surrogates for cyber power. Analysis of each paradigmatic school of thought will aim to expose the perils inherent in each theoretical broad path, and thereby help to better define the relationships between cyber's competing core roles. In turn, a surrogate theory, if built upon a broad awareness of these perils, can help free leadership to focus on the many challenges that rest within cyber power's higher realms.

At the micro level of this thesis' analysis, Khong's AE Framework demands that a list of possible cyber regents be drawn up. Many of air power's roles, as has been demonstrated, first emerged during the cauldron of hostilities of World War I. It is not surprising therefore that air power's intellectual leadership including Douhet, Mitchell, Trenchard, and Slessor, reflecting upon this experience, came to the fore in the respite of the interwar period.[6] Aware of the risk of reductionism and over-polarization of the argument, this thesis suggests that air power's founding fathers can be gainfully analyzed by dividing them into two broad paradigmatic schools that dominated air power's

[5] Clausewitz, *On War*, 578.
[6] Mueller, *Air Power, 2.*

formative era of cognitive and organizational development: a Douhetian paradigm and a Slessorian paradigm.[7]

The Douhetian paradigm is founded upon the promise of air power to bypass an enemy's armed forces and strike at the heart of society or leadership.[8] Groves captured the implication of the Douhetian paradigm perfectly: air defense was regarded as inefficient folly.[9] Consequently, as Douhet proposed, one should resign oneself to submit to attack, to better employ all possible means for launching one's own great offensive.[10] The only logical course that a nation could employ, if it was a student of the Douhetian school of thought, would be a "policy of aerial offensive-defense": a policy dominated by the unleashing of air power's deep strike capability against the "heart and nerve centers" of its enemy.[11] This paper therefore suggests that the adversary, in the Douhetian paradigm, is not represented as an enemy's fielded forces but rather as a societal network of networks akin to Lord Tiverton and Gorrell's early articulation of industrial web theory.[12]

In contrast to the Douhetian paradigm, the Slessorian school of air power theory does not focus upon society or industry as a singular, all-dominating center of gravity, but instead, presents a more multi-faceted and nuanced picture of air power's key roles. Proponents of the Slessorian paradigm emphasize that the "first and foremost" commitment of an air force is the defense of one's own nation against air attack.[13] Intimately connected with this commitment is the provision of air force elements to co-operate with its sibling services in theatre: counter-domain roles are therefore emphasized

---

[7] The term "Douhetian paradigm" of air power has been widely employed in air power analysis and also in terms of information warfare. See for example, Michael Brown, "Information Warfare and the Revolution in Military Affairs", *Seminar on Intelligence, Command, and Control, Guest Presentations*, Spring 1995, 13-14.

[8] For the purposes of this paper, Douhet, Trenchard and Mitchell are considered as versions of the Douhetian paradigm.

[9] P.R.C Groves, "England Without a Defence," *The Times*, London, 21 March 1922 and 24 April 1922 reprinted in Emme, *The Impact of Air Power* (Princeton: Van Nostrand, 1959), 177-179.

[10] Douhet, *The Command of the Air,* 109.

[11] Groves, *England Without a Defence*, 177-179.

[12] For an excellent description of the emergence of industrial web theory see Biddle, *Rhetoric and Reality in Air Warfare,* 130-131.

[13] Slessor, *Air Power and Armies*, 1.

before deep strike.[14] In representing the enemy's center of gravity as the decisive defeat of his fielded armed forces, the Slessorian School is presented as being akin to an air power annex to Clausewitz's *On War*.[15]

If air power theory is to help guide the UK and US's preparation for cyber war, should a more Douhetian philosophy be adopted? What perils lie in wait on a path that accepts Denning's assertion that there is no silver bullet against cyber assault, and leads nations to decide that minimal military means should be diverted from launching offensives against the enemy?[16] Or should Slessor guide cyber's strategic hand? A path grounded in the recognition that a nation must be prepared to parry an adversary's cyber blows if it is to be left with the means to strike back with its military forces?[17]

Bypassing the Conventional War – The Perils of a Douhetian Cyber Paradigm

Molander predicted that the evolution of strategic warfare would "include a dimension of cyberspace threats and vulnerabilities worthy of the label strategic information warfare."[18] This thesis concurs with Freedman's excellent argument that to label any form of war as strategic is nonsensical: strategy is a feature or war, rather than a type of warfare.[19] To label cyber power a strategic form of warfare is therefore not only guilty of insidious analogy, but also flawed understanding. Information warfare, as Libicki states "only looks strategic."[20] In actuality, the term strategic information warfare, like strategic bombardment and strategic air power before it, applies to nothing more than a function: cyber power's deep strike ability to bypass the conventional battlefield and potentially strike at the heartland of the enemy via the Fifth Battlespace. This thesis therefore concludes that the term strategic must never be employed in the cyber lexicon to describe any Fifth Battlespace function. But cognizant of the ill-titled nomenclature of strategic information warfare, the role it represents is characteristic of the features of a Douhetian cyber paradigm and hence must be considered here.

---

[14] Slessor *Air Power and Armies,* 79-80.
[15] Clausewitz, *On War*.
[16] The author notes that Denning is also guilty of mixing her metaphors somewhat: surely a more apt term for a panacea defensive solution would be a silver shield, rather than bullet. Denning, *Information Warfare and Security*, xiv.
[17] Paraphrased from Clausewitz, *On War*, 309.
[18] Molander, *Strategic Information Warfare: A New Face of War*, 2.
[19] Freedman, *The Evolution of Nuclear Strategy*, 112.
[20] Libicki,. *Conquest in Cyberspace*, 37.

Whilst Molander's predictions for cyber power have not yet come to pass in terms of demonstrated military experience, cyber power's deep strike role has certainly come to exist in terms of expectation, and of perceived threats and vulnerabilities.[21] The problem herein for this analysis is how to assess the potential of a Douhetian cyber paradigm without the crucible of experience to expose the strengths and weakness of such a path. Rattray's work provides a solution. In his book *Strategic Warfare in Cyberspace*, Rattray derived enabling conditions for strategic air warfare.[22] If these conditions are applied to contemporary cyber power, they could expose the strengths and weaknesses that are presented by the adoption of a Douhetian preference towards deep strike. Foremost among these enabling conditions were: a demonstrable offensive advantage; and the existence of an exploitable vulnerability in the selected center of gravity.[23]

First, considering cyber power in terms of offensive advantage, Cornish emphatically states that cyber warfare demonstrates "offensive dominance."[24] As a strategic method, he concludes that offensive cyber action is easier, quicker and usually cheaper than defensive action. But this analysis cites the unfounded assertions of cyber practitioners and advocates such as Miller who foretell that it would take just two years, less than $50 million, and only 600 personnel to paralyze the US by cyber attack.[25] Such categoric numerical prediction resembles Douhet's analysis of the "Martyrdom of Treviso" to demonstrate the destructive capacity of air power.[26] But finding exploits in MacBooks and iPhones does not represent a cyber equivalent to Douhet's images of explosive, incendiary and poison-gas bombardment.[27] Neither Miller nor Cornish

---

[21] This thesis acknowledges isolated fledging deep strike examples such as the recent Stuxnet assault upon Iran. However, cyber power is all-too-often represented as a cheap and easy means to political ends without supporting evidence. For example see Michael Smith, "General Sir David Richards Calls for New Cyber Army, *The Times*, 17 Jan 2010.

[22] Rattray, *Strategic Warfare in Cyberspace*, 77-151.

[23] Rattray, *Strategic Warfare in Cyberspace*, 288.

[24] Cornish, *On Cyber Warfare*, 28.

[25] Charlie Miller, "Time to Wake Up To Cyber Threat," *Space War.* http://www.spacewar.com/reports/Time_to_wake_up_to_cyber_threat_experts_999.html (accessed 12 April 2011).

[26] Douhet, *The Command of the Air*, 23-24.

[27] Beagle and Libicki both reflect that air power's targeteers often overstated how long enemy infrastructure would be unavailable if destroyed. The relevance of this observation to cyberspace is that it is a far more difficult environment in which to make such calculations. Miller's paralysis, even if

demonstrate how such attacks would scale up to paralyze a nation; nor do they explain the mechanism by which ultimate achievement of political ends is accomplished via purely offensive cyber means.[28]

Air power's freedom of action led to the offensive advantage of the aerial weapon being regarded as the *primus inter pares* principle of the Douhetian paradigm.[29] But as Douhet's analysis demonstrates, it is easy to overstate the effects that freedom of action can achieve. Moreover, it is easy to overlook Clausewitz's warning that war is not an exercise of the will directed at the inanimate matter of buildings and industry; or hardware and software.[30] A constant in the nature of cyber war, as it is in war from the air, is that will is still directed at an animate enemy who reacts.

History demonstrates that air power's Douhetian school oft underestimated the animate nature of an adversary, evidenced in the form of the impact of defensive innovations: radar; radio; the Royal Observers Corps; and high performance pursuit aviation were all combined to deadly effect in Dowding's air defense "systems of systems."[31] And Douhet, who repeatedly asserted that "the use of antiaircraft guns is a waste of energy and resources,"[32] may have been forced to surrender this stance in light of the devastating losses that British and American crews suffered over German cities.[33] Whilst the physical destruction of offensive cyber forces is not likely to be a primary means of reducing a cyber offense's freedom of maneuver, the import of the anomaly of defensive innovation must augment any Douhetian-oriented cyber paradigm.[34] Cyber

---

achievable, is therefore likely to be temporary in nature. Libicki, *Cyber Deterrence and Cyber War*, 55. and T W Beagle, *Effects-Based Targeteting: Another Empty Promise?* Air University, June 2000.

[28] In 2008, Miller won a hacker conference competition for being the first to find a critical bug in a MacBook. In 2009, Miller demonstrated an SMS processing vulnerability that allowed Apple iPhones to be compromised.

[29] Mueller, *Air Power*, 2-5.

[30] Clausewitz, *On War*, 149.

[31] Bungay, *The Most Dangerous Enemy: A History of the Battle of Britain*, 47.

[32] Douhet, whilst acknowledging the improved range and accuracy of antiaircraft guns, refused to amend the validity of this statement. See footnotes in Douhet, *The Command of the Air*, 55.

[33] Randall Wakelam, *The Science of Bombing: Operational Research in RAF Bomber Command* (Toronto: University of Toronto Press, 2009), 157-182 and Dana Johnson, *Roles and Missions for Conventionally Armed Heavy Bombers – A Historical Perspective* (Santa Monica, CA: RAND, 1994), 20.

[34] Anomaly subverts accepted practice and demands the reconstruction of prior assumptions, the re-evaluation of prior facts, and is strongly resisted by the established community. Any Douhetian-oriented

power's dynamic defensive capabilities will continue to evolve: intrusion detection systems and network monitoring tools, akin to a cyberspace radar, will improve an adversary's defensive situational awareness in the Fifth Battlespace; and anti-malware and boundary protection devices, analogous to digital antiaircraft batteries, will perpetually develop and increase the chances of offensive forces being intercepted. Theory, if it is to be useful, demands a degree of longevity. The dynamic nature of the cyber domain, even if cyber power is assumed to have offensive dominance at present, does not guarantee that the relationship between offense and defense cannot be reversed via defensive innovation. The offensive dominance characteristic of cyberspace, if it exists, must therefore be acknowledged to be a temporal feature that must be revisited and re-evaluated within each generation's contemporary context.

Even when freedom of maneuver has been established, air power's history reminds advocates of the Douhetian paradigm that some centers of gravity demonstrated very limited vulnerability to aerial bombardment: the need for constant vigilance regarding the fungibility of the offensive military cyber instrument is highlighted herein.[35] For example, Murphy stylizes the cyber attack on Estonia as Clausewitzian, in the sense that its intent was to create mass social panic.[36] This thesis suggests that the employment of cyber power in Estonia, if its ends were to achieve victory via mass social panic misrepresents Clausewitz, and is instead a contemporary equivalent of Trenchard and the Douhetian paradigm.[37] Sympathetic readers of Murphy and Miller should reflect that Trenchard's "twenty to one" assertion, regarding the ratio of moral to material effect of aerial bombardment, has proved to be unfounded.[38] Moreover, aerial bombardment's inability to fashion the moral of a populace into a targetable center of gravity had long been predicted. Indeed, Churchill himself presented on the improbability that air attack,

---

cyber paradigm that does not reflect the existence of this anomaly from the outset, even if able to evolve, is likely to waste significant resources in the long-term. Kuhn, *The Structure of Scientific Revolutions* , 6-7.

[35] Rattray, *Strategic Warfare in Cyberspace* 290.

[36] Murphy, *Attack or Defend*, 91.

[37] Trenchard's "relentless offensive" bias regarding fragility of social order is demonstrated in the following quote: "It is too easy to lose sight of the effect one is making if one is too anxious to safeguard oneself from attack…Our people would undoubtedly squeal if they were bombed, but we should find, if we bombed the enemy enough, that he should collapse before we did." Quoted in Biddle, *Rhetoric and Reality in Air Warfare,* 85.

[38] Biddle, *Rhetoric and Reality in Air Warfare,* 79.

aimed at a civilian populace, would compel a nation to surrender and could instead harden the resolve a people's combative spirit.[39] Is it realistic to expect that if the firestorms of Dresden could not crush the spirit of the German people, surely even the most all-encompassing cyber assault would struggle to paralyze the UK or US? Libicki's analysis proves that whilst living in a world without electricity, telecommunications or financial services is "wearing after a while," such hardships are not, by themselves, fatal to human survival or an orderly society.[40] This conclusion will be revisited in the next chapter's consideration of the limitations of independent cyber action, but in the context of the current dimension of analysis, it also ably serves to demonstrate that the over-expectation of cyber power's efficacy must be guarded against if a Douhetian paradigm is adopted.

Douhetian disciples may therefore consider that the societal network of networks against which cyber power is best suited is instead the industrial and economic web. Indeed, a great many pages of cyber literature have been dedicated to describing the paralyzing effects of an attack on Wall Street or the London stock exchange.[41] Experience would also seem to support that a cyber adversary may attempt to exploit such a threat vector. For example, many of the 2007 attacks on Estonia were targeted at its financial institutions.[42] But post-World War II analysis of the economic effects of aerial bombardment may contain a useful cautionary tale for cyber strategists tempted by this line of argument: a cautionary tale that has led many authors to concur with Arthur

[39] Winston Churchill, "Munitions Possibilities of 1918", 21 October 1917 printed in H A Jones, *The War in the Air: Appendices* (Oxford: Oxford University Press, 1937),18-21.
[40] Libicki, *Conquest in Cyberspace*, 43.
[41] For example, witness McCarthy, Burrow, Dion and Pacheco's analysis of the "February 2007 Dow Jones' glitch": a one hour delay in calculating the Dow Jones Industrial Average occurred due to an unprecedented volume of trade on a chaotic day in the markets in late February 2007. When stand-by trading systems were activated, the Dow Jones' Industrial Average rapidly caught up with the back-log and gave the impression that markets had suffered an instantaneous 200 point further drop, which in turn induced some further panic selling. What such accounts fail to note is the crucial fact the majority of the day's drop was not due to the computer error but normal trading in a panicky market. Nor do they note that there were no long-term macro effects akin to a cyber-induced economic paralysis. Kramer, *Cyberpower and National Security,* 547-548; and Denning, *Information Warfare and Security,* 72-73.
[42] Cornish, *On Cyber Warfare,* 5.

Harris that no German economic "Achilles heel" existed.[43] The panacea of a vulnerable industrial network of networks, that would unravel Hitler's war machine by simply unpicking a few key stitches, did not materialize.[44]

Analysis of the Allies' protracted aerial assault exposes the unexpected degree of resilience, spare capacity and reserves Germany possessed that helped dissipate the anticipated strategic effects. Indeed, the British Bombing Survey reported that German war production losses via aerial bombardment were only around one percent.[45] Coincidently, analysis of the economic impact of cyber attacks shows that targeted firms tend to suffer losses of a similar factor: in the region of one to five percent.[46] Moreover, these losses are soon recovered because as Bassett notes "in mounting an advanced cyber-attack, the perpetrators reveal their methods and techniques and thus provide the defender with the means to evolve effective counter-measures. A stock exchange with a robust approach to resilience and a strong event management structure should be able to recover effectively from anything other than a catastrophic first strike."[47] If air power is to act as cyber power's guide, history would suggest that the probability of such a catastrophic strike is exceedingly low: "whatever the target system, no indispensable industry was permanently put out of commission by a single attack. Persistent re-attack was necessary."[48] The lesson herein for cyber power is that although offensive advantage may be leveraged, the effects that can be achieved from that offense may be significantly lower than anticipated. The enemy is animate and his cyber efforts to react to, and recover from, an economic cyber assault may prove more robust and efficient than the ISR and deep strike cyber resources required to launch and sustain such an assault. The intelligence and offensive resources demanded should also not be underestimated, for as

---

[43] Arthur Harris repeatedly employed the phrase "panacea targets" as a pejorative term. For example, see Miller's account of Harris' reaction to Tedder's Transportation Plan, Donald Miller, *The Story of World War II,* (New York, NY: Simon & Schuster, 2001), 279.

[44] Pape, *Bombing to Win*, 258-260.

[45] *United States Strategic Bombing Survey (USSBS) Summary Report (European War),* 4-15; *British Bombing Survey Effects on German Towns*, 40.

[46] Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, *The Economic Impact of Cyber-Attacks*, 1 April 2004. 2.

[47] For example, see John Bassett and David Smart, "Cyber-attacks on the Stock Exchange: Threat, Motivation and Response," *RUSI On-line.* http://www.rusi.org/go.php?structureID=commentary&ref=C4D4AD93B92E87, (accessed 27 March 2011).

[48] *USSBS Executive Summary*, 17.

Pape posits, if an economic strategy is to have any chance of success, reliable economic metrics from across the target industry must be available and monitored to determine the efficacy of the targets being attacked.[49] Applying this logic to the context of cyberspace, once hostilities are launched, such information is unlikely to be easily available as an adversary's virtual drawbridges are raised.[50] The cyber role of ISR is therefore a crucial pre-requisite for successful deep strike operations in the Fifth Battleapce.

The perils inherent in a Douhetian cyber paradigm have been demonstrated to be legion; however, the fifth aspect of Khong's AE Framework, that of ethics and the evaluation of "moral rightness," also demands consideration at this point.[51] Adams adopts a Trenchardian tone when suggesting that "private citizens are on the front line of twenty-first century warfare.[52] Clarke goes further in his assertion that "the most likely targets" in a cyber war will be civilian.[53] Moreover, referring to the National Military Strategy for Cyber Operations, he contests that this ethical pitfall remains open because civilians have not been declared "off limits" to offensive cyber operations.[54] To accept Clarke's conclusion is to ignore the tome of Western academic and political study that has been devoted to the development of legal frameworks to govern offensive cyber power.[55] But cyber space's deep strike role certainly has the potential to represent a contemporary equivalent to Freedman's recognition that strategic bombardment was defined by "a blurring of the targeting boundaries between the military and civilian spheres of society"; a blurring that this paper suggests was not resolved with the cessation of hostilities.[56]

---

[49] Robert Pape**,** *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 275.

[50] For example, many crucial product engineering portions of organizations' information infrastructures are already air-gapped. See Libicki, *Conquest in Cyberspace*, 64 and 106.

[51] Khong, *Analogies at War*, 22.

[52] James Adams, "Virtual Defense," *Foreign Affairs*, (May/June 2001): 98-112.

[53] Clarke, *Cyber War: The Next Threat to National Security and What to Do About It,* xi.

[54] Clarke, *Cyber War: The Next Threat to National Security and What to Do About It,* 45.

[55] See for example Owens et al substantial analysis and recommendations that cyber attack should be judged according to the existing principles of the Law of Armed Conflict and the UN Charter, thus encompassing both *jus ad bellum* and *jus in bello* principles until specific regulations are drawn up that apply to cyber weapons. *Cyberattack Capabilities*, 239-292.

[56] Freedman, *The Evolution of Nuclear Strategy*, 113.

After World War II, the Strategic Bombing Survey specifically recommended that targets should be selected that were difficult to disperse or harden.[57] But the Fifth Battlespace, by its layered nature, is likely to see significant portions of military cyberspace dispersed and hardened.[58] If legitimate military information infrastructure targets become harder to attack, Adam's conclusions may appear more palpable: cyber power could be considered against the archipelagoes of vulnerability that have least flexibility in terms of responsiveness and recovery options.[59] Such targets include Air Traffic Control systems, and national power generation systems,[60] so often cited by cyber's "Cassandras" as potential targets today.[61] Whilst the UK and US may consider the employ of cyber power against such targets as a gross defilement of the ethical principles of war, Freedman's consideration of air power's development leads him to the conclusion that a preoccupation with new offensive means has sometimes resulted in too little consideration of the purposes for which such means might be employed.[62] Could the gravitational pull of cyber's deep strike role prove as irresistible as Gavotti's marriage of the airplane and the bomb?[63] Whilst the answer to such a question is known only to the future, one thing is certain: it is the military that will be charged to council political leaders regarding cyber power's deep strike role. This thesis asserts that the burden of responsibility must fall upon the shoulders of military cyber leaders to protect against the Douhetian allure of the "technological sublime,"[64] and the pitfall of ethically questionable

---

[57] *USSBS Executive Summary*, 16.

[58] Recall this paper's definition of cyberspace as an inherently layered domain in which "archipelagoes of strictly-bounded connectivity may exist."

[59] Rattray, *Strategic Warfare in Cyberspace,* 291.

[60] Robert A.Miller and Irving Lachow. "Strategic Fragility: Infrastructure Protection and National Security in the Information Age." *Defense Horizons* (Center for Technology and National Security Policy, National Defense University) No. 59, January 2008.

[61] Richard Clarke employs the term Cassandra with reference to cyber doom-mongers that mayt speak the truth but are damned never to be believed. For example: Larissa Paul, "When Cyber Hacktivism Meets Cyberterrorism," *SANS Institute*, February 19, 2001 "Examples of cyber terrorist actions can include hacking into an air traffic control system that results in planes colliding…"; Information Assurance Task Force of the National Security Telecommunications Advisory Committee. http://www.aci.net/kalliste/electric.htm ; and O'Neill in *Cyberpower and National Security*.

[62] Freedman, *The Evolution of Nuclear Strategy*, 46

[63] De Groot, *The Bomb: A Life*, 2.

[64] The term "technological sublime" was coined by Perry Miller to describe a common feeling of awe, inspired by large-scale applications of technological prowess. For more details see David Nye, *American Technological Sublime* (Cambridge, MA: MIT Press, 1994).

cyber employ that lies therein.[65] Any theory of cyber power must therefore be mindful of Churchill's reflection: "The destruction of Dresden remains a serious query against the conduct of Allied bombing . . . I feel the need for more precise concentration upon military objectives, such as oil and communications behind the immediate battle-zone, rather than on mere acts of terror and wanton destruction, however impressive."[66]

Power to the Edge – The Perils of a Slessorian Cyber Paradigm

Churchill's emphasis that air power should concentrate upon military objectives within the "immediate battle-zone" chimes with the core tenets of this thesis' Slessorian paradigm: air force elements co-operating with sibling services to defeat an enemy's army in theatre, not merely by striking tactical formations, but also via interdiction.[67] Patrick, an American founding member of the Slessorian school, commented that the major functions of military aviation should be to: assist the ground forces by destroying enemy air forces; attack enemy ground and maritime forces; and protect oneself from enemy attack.[68] Both Slessor and Patrick therefore are presented as placing a common emphasis upon the defensive role that air power has to play; augmented by an offensive role primarily founded in the functions of counter-air and counter-land operations.[69]

Considering first the Slessorian emphasis upon defense, this thesis has suggested that air power and cyber power both serve as contemporary metaphors for Siena's walls: the challenge to a state's ability to maintain and secure its borders.[70] For Lorenzetti's Allegory of Good Government to be realized, defensive efforts to secure Siena's walls must be attempted if internal discord is to be averted.[71] This is a challenge that a

---

[65] Kramer, *Cyberpower and National Security*, 316-318;

[66] Winston Churchill's memo to Charles Portal, 28 March 1945. Under pressure from Air Chief Marshal Arthur Harris and Portal, Churchill withdrew this memo, issuing a revised version on 1 April 1945 omitting the words "acts of terror."

[67] Slessor, *Air Power and Armies*.

[68] General Patrick, Fort Leavenworth Lecture, 27 March 1924, in General Patrick's National Archives File, Records of the Air Service, 1917-1926, quoted in Greer, *The Development of Air Doctrine in the Army Air Arm, 1917-1941*, 1955.

[69] It is important to note that neither Slessor nor Patrick were opposed to the concept of air power's deep strike role. In fact, both were keen advocates of this capability; however, they were prepared to challenge its over-arching import within the air power portfolio.

[70] Omand, *Securing the State*, 1-2.

[71] Omand, *Securing the State*, 92-93.

Douhetian "offensive-defense" strategy fails to satisfy:[72] cyber offense does not demonstrate to a population that the immediate cyber integrity of the state is being defended. A Slessorian emphasis upon the import of cyber defense, and demonstrated control of friendly cyber space, would seem to negate this risk. But Denning is correct in her assertion that there is no single silver bullet against cyber attack. The strength of a Slessorian cyber paradigm is that neither does there need to be! [73] Slessor stated that it is impossible to deny the air to a determined enemy.[74] But he also recognized that the Gothas' bombing of London could not have led to defeat of British forces in the field. Instead the Gotha raids represented a political risk that the Government would be perceived as leaving London unprotected.[75] History demonstrates that societies can be remarkably hardy centers of gravity, as long as it can be demonstrated that defensive efforts are being made. As Michael notes, the defensive cyber arena has become a highly politicized problem space: as such it mirrors air power's experience in 1917.[76] The defensive role of air power in the Slessorian paradigm is therefore not to overwhelm itself by seeking to craft a silver bullet of cyber defense that can protect all facets of society, but instead to satisfy the political demand that sufficient effort is being made. Consideration of a Slessorian paradigm also exposes the requirement for any cyber lexicon to better facilitate the articulation of defensive cyber efforts to the populace writ large.

But the danger posed by the political fear of a cyber breaching of Siena's walls presents a most pertinent risk if a more Slessorian-influenced paradigm is adopted. General Kehler stated that "The offense always has a strong advantage, overwhelming, subverting, or defeating static defenses."[77] In contrast, Libicki when considering the

---

[72] Neither is it authorized to do so under current legislation. As General Keith Alexander noted on 30 March 2011: "We don't have the authority to stop an impending cyber attack [via pre-emptive cyber means.]" Defense is therefore demanded in any theory of cyber power if it is to serve its political master.
[73]Dorothy Denning, *Information Warfare and Security* (New York, NY: ACM Press, 1999), xiv.
[74] Slessor, *Air Power and Armies*, 19.
[75] Slessor, *Air Power and Armies*, 17.
[76] Alex Michael, *Cyber Probing: The Politicisation of Virtual Attack* (London: Ministry of Defence, 2010), 1.
[77] General Kehler, "Testimony to Senate Committee on Armed Services," *Airforce Magazine*, 29 March 2011, http://www.airforce-magazine.com/SiteCollectionDocuments/Testimony/2011/March%202011/032911kehler.pdf, 15. (accessed 1 May 2011).

passive defensive strength that the cyber domain can demonstrate, suggests that system administrators can apply the "blunt" tools of physical control to ably protect an information infrastructure under siege: fiber and wire connections can be severed; electromagnetic emissions can be jammed; hard-tokens and biometric access measures can be strictly employed; and manual over-ride measures can be designed into any system.[78] The danger herein for a graduate of the Slessorian school is not that Siena's cyber walls will fail because they are weak; or that like the Maginot Line, they will fail because they are static; instead, the paradox that exists for a theory of cyber power is that defenses will fail if they are built too securely.[79] A Slessorian paradigm must therefore guard against defensive over-reaction if that over-reaction serves to cripple one's own freedom of maneuver in the Fifth Battlespace, and thus undermines the effects that leveraging of cyberspace is facilitating in the world beyond Siena's walls.

This thesis turns now to consider Slessor's argument that control of the air was simply a stepping stone to facilitate the leveraging of air power's counter-land role to strangle and decisively defeat an adversary's land forces.[80] If cyber warriors are to fulfill their destiny as the "midwives of victory," any Slessorian paradigm must also recognize that delivery of military success will ultimately be facilitated by information-enabled sibling services in the physical domain.[81] A peril inherent in such a philosophy is that military cyber power is presented in a predominantly auxiliary role, the negative connotations of which will be considered in the next chapter. But within the current analysis of the perils of a Slessorian paradigm, placing too great an emphasis upon cyber power's enabling role, to support counter-land operations and its sister domains, also poses the danger of striking a most Faustian of bargains.[82]

---

[78] Libicki, *Conquest in Cyberspace*, 66-67.

[79] General Kehler recently noted: "Cyberspace is dynamic, and specific threats require specific countermeasures. The Maginot Line failed because it was static and the defense failed to anticipate and address technological and tactical changes." "Testimony to Senate Committee on Armed Services," *Airforce Magazine*, 29 March 2011, http://www.airforce-magazine.com/SiteCollectionDocuments/Testimony/2011/March%202011/032911kehler.pdf, 15. (accessed 1 May 2011).

[80] Slessor, *Air Power and Armies*, 8-10.

[81] Gray, *Modern Strategy*, 36.

[82] The legend of Faust tells of a highly successful, yet overly ambitious academic who surrenders his moral integrity by striking a deal with the devil that exchanges his soul for infinite knowledge and success.

As Alberts and Hayes note, "power to the edge" organizations seek to become more powerful by bringing all of their information and military assets to bear upon an adversary.[83] But herein rests a further paradox inherent in cyber power: the more information is leveraged by its sister domains, so the potential to introduce new vulnerabilities and dependencies also increases. As the Tofflers correctly observed, "the sword of knowledge cuts two ways."[84] So like Faust, if UK and US NCW-era forces are overly ambitious and transformational in seeking to become Slessorian "power to the edge" organizations, they may well do so at the cost of surrendering their own cyber integrity. A military over-reliance upon cyber power to facilitate operations could become a Clausewitzian Centre of Gravity: not from an adversary's making, but from our own unchecked ambition. A Slessorian cyber paradigm that becomes overly offense-oriented in terms of its auxiliary role must be cognizant of this dynamic. Failure to do so ignores that risk that Munro highlights: an over-leveraging of information, coupled with the fragility of cyber power, could witness a numeric superiority of one hundred to one change on the turn of a fuse.[85]

Conclusions

This chapter has defined and analyzed two broad paradigmatic schools of air power theory: a Douhetian paradigm; and a Slessorian school of thought. The guiding hand of each of these air power bodies of opinion has been analyzed, and their utility to help safely steer cyber power's pressing development requirements considered. But Gray reminds us that the allure of any guiding theory to "capture the minds of supposedly practical people should not be underestimated."[86] The perils inherent in the application of a wholly Douhetian or Slessorian cyber paradigm have therefore been emphasized.

Analysis of a Douhetian paradigm has identified numerous pitfalls that any guiding theory of cyber power should seek to avoid. First, it has been contested that the offensive dominance of cyber power's character cannot be assumed. As Lonsdale succinctly notes, cyber power's future must be grounded in contemporary reality: "Future

[83] David Alberts and Richard Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, D.C.: Command and Control Research Program, 2003), 213.
[84] Toffler, *War and Anit-war*, 147.
[85] Neil Munro, *The Quick and the Dead: Electronic Combat and Modern Warfare* (New York, NY: St Martins Press, 1991).
[86] Gray, *Modern Strategy*, 35.

force structure, doctrine, strategy and general preparation for war should reflect the nature of warfare and not some idealized vision of potential."[87] Cyber power's future offensive capability therefore cannot be assumed to be a linear extrapolation of the limited contemporary capabilities and vulnerabilities currently demonstrated. Neither must any guiding theory be founded upon the erroneous assumption that the will of an information age populace can be fashioned into a cyber-assailable center of gravity. A similar risk of over-expectancy, in terms of the existence of panacea industrial or economic targets, has also been exposed. The enduring value of Clausewitz's counsel has been demonstrated by iterating that the cyber adversary is not a fleeting technical exploit that hides within networks, hardware and software; but rather the enduring animate and thinking enemy. The man-made nature of the cyber domain may therefore tend to favor defensive innovation, and consequently any offensive cyber advantage can only be assumed to be temporal in nature. This thesis has also demonstrated that the Douhetian allure of the "technological sublime," and the pitfall of ethically questionable use of cyber power, presents a very real risk that military cyber leadership and a theory of cyber power must protect against.

In considering the Slessorian paradigm, this thesis has taken fundamental issue with digital Douhetians such as General Elder who categorically assert that "If you are defending in cyberspace, you're already too late."[88] Siena's cyber walls will not fail because they are, on occasion, penetrated; or that like the Maginot Line, they will fail because they are static; instead, the paradox that must be factored into any future theory of cyber power is that cyber defenses will fail if they are built too securely, or hidden behind for too long. As Libicki cautions, a cyber strategy that keeps its enemy ensconced behind its own walls has won freedom of the agora.[89] A Slessorian cyber paradigm has also been argued to rest upon the recognition that delivery of military success will ultimately be facilitated by information-enabled sibling services in the physical domain.[90] The Faustian bargain that Slessorian "power to the edge" cyber forces must resist is that

[87] Lonsdale, *The Nature of War in the Information Age*, 95.
[88] Clarke, *Cyber War: The Next Threat to National Security and What to Do About It,* 36.
[89] Libicki, *Conquest in Cyberspace*, 62-64.
[90] Gray, *Modern Strategy*, 36.

of being overly ambitious and transformational, because the price of excessively leveraging cyber power may well be surrendering of one's own cyber integrity.

If air power's experience has demonstrated one certainty for a theory of cyber power it is that air power's theories were inconclusive. This is not due to a lack of evidence or study, but simply that war is the most wicked and interrelated of problem spaces. Advocates of both the Douhetian and Slessorian paradigms can espouse a role in delivering victory. As Weigley succinctly concludes: "the ground and aerial campaigns…were so closely interdependent that is impossible to judge what either of them might have accomplished if unassisted by the other."[91]

This thesis suggests that the peril of competing paradigms, and overly-polarized theorists like Denning, is not that one will select the incorrect air power paradigm to apply to help identify cyber power's best path. The peril of competing paradigms is succumbing to the perception of mutually exclusivity.[92] This chapter has demonstrated that the pitfall of digital analogical reasoning can trap the unwary traveler on the path of cyber power's development if they seek to adopt a single surrogate air power theory and in doing so, fail to learn from the breadth of air power's rich, and at times, painful experience. The ultimate peril of competing paradigms therefore is the danger of filling cyber power's cognitive void with a single absolute: Starr's demand for a comprehensive and robust theory.[93] A degree of ambiguity, whilst unsatisfying to strategists seeking topiary perfection in Clausewitz's "hedges of principles," may better serve cyber power's contemporary guiding needs.

From the Slessorian school of thought, cyber power's defensive role has been emphasized if one seeks to guarantee one's own freedom of maneuver in the Fifth Battlespace; and support cyber-enabled sibling services in the physical domain. Control of cyberspace therefore assumes the enduring priority role in any theory of cyber power. From the Douhetian school, cyber power's deep strike role has been demonstrated to be dependent upon ISR support, and hence an emphasis upon deep strike without an appreciation of its symbiotic dependency upon its enabling cyber roles is also presented

---

[91] Russell Weigley, *The American Way of War: A History of US Military Strategy and Policy* (Bloomington: Indiana University Press, 1977), 358.

[92] This thesis interprets Kuhn to posit that multiple paradigms can co-exist.

[93] Starr, *Toward a Preliminary Theory of Cyberpower,* 44.

as folly. This thesis, in describing these relationships, therefore concludes that any surrogate theory of cyber power must support a balanced cyber portfolio, albeit placing emphasis upon control of cyber space as the *primus inter pares* of cyber's roles. But as the next Chapter will demonstrate, air power's organizational issues can divert theory from the path of analytical purity. Consideration of Gray's organizational dimension of strategy is therefore also demanded.

Chapter 5

THE STRATEGIC DIMENSION OF ORGANIZATION – THE ATHENA SYNDROME

Cyber operations may hatch and be fed within the Air Force's nest, but in the future, the Air Force will need to push cyber operations from its nest so it can fly as the Cyber Force.

-- Natasha Solce

Air power is one piece, the profession of arms is the other. One is the heart of the Air Force, the other is its soul.

-- Carl Builder [1]

Air power theory, through the stereoscopic lenses of this thesis' Douhetian and Slessorian paradigms, has been analyzed to provide a strategic depth of vision to help inform and safely guide cyberpower's interim development. Each of these contrasting perspectives has highlighted numerous pitfalls that a theory of cyber power must avoid. It must, however, be recognized that Gray's strategic dimension of theory is but one facet of a model: a model that is built upon well-informed, but ultimately arbitrary divisions.[2] As Mueller rightly notes, air power's leading theorists were also influential advocates of military aviation.[3] The rich intellectual legacies which helped expose the potential of air power cannot be decoupled from the historical context in which they were born. This thesis' macro-level framework has been crafted to reflect that no balanced analysis can ignore the fact that air power's intellectual founding fathers also sought to garner interest and investment for air power in a period of harsh fiscal climes, and in the face of stiff

---

[1] Carl Builder, *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and Fate of the U.S. Air Force* (New Brunswick: Transaction, 2009), xvii

[2] The author wishes to emphasize that the term arbitrary is not employed in the sense of capricious, unsupported delineation and in no way represents a criticism of Gray's outstanding model. The term is instead employed in the sense of discretionary judgment, whilst also highlighting that no model can perfectly reflect reality. For example, just as biochemistry spans the arbitrary scientific divisions of chemistry and biology, so some significant air power issues span more than one of Gray's dimensions of strategy. Peter Checkland, *Systems Thinking, Systems Practice* (Wiley), 4.

[3] Karl Mueller, *Air Power,* RAND, 2010. http://www.rand.org/pubs/reprints/2010/RAND_RP1412.pdf (accessed 15 February 2011).

organizational resistance from extant military services.[4] Thus, any consideration of air power theory cannot be divorced from a similar examination of Gray's strategic dimension of organization.[5]

The RAF and the USAF, hatched and fed by in the nest of the Army and the Navy, both stretched their wings and flew to meet their destinies as independent military services.[6] But the debate regarding independence has been a perpetual and, at times, strategically perilous distraction for air power's leadership: an ongoing organizational influence that some have coined the Icarus Syndrome.[7] Does a similar malady await cyber power? A condition that this thesis shall call: the Athena Syndrome. This thesis suggests that a symptom of the Athena Syndrome is tunnel-vision, induced by too great a focus upon independence. Untreated, the Athena Syndrome carries with it a significant risk that cyber-leaders may stray from the path of strategic efficacy, lured instead by a path to organizational independence. To paraphrase Builder: "Cyber power is one piece, cyber professionalism-at-arms is the other. One is the heart, the other the soul."[8] The challenge facing cyber power's leadership is how best to nurture both heart and soul. The danger of misapplied strategic analogy is the Khongian risk that the price of cyber power's independence will be at the cost of its soul: a corruption of cyber's professionalism-at-arms. It is hoped that reflection upon air power's experience will help immunize cyber power against the ill-effects of such an infection. In turn, this analysis will demonstrate that a new form of advocacy is demanded for cyberspace. Cyber power's Douhets and Mitchells must be muted.[9] Advocacy born in the fictional realm of

---

[4] Numerous authors have written upon the intense intramural battles that have accompanied the formation of the RAF and USAF as independent air forces. For example, see Jeffrey Barlow, *Revolt of the Admirals* (Washington D.C.: Naval Historical Center, 1994).

[5] Gray, *Modern Strategy*, 33-34.

[6] The RAF was formed on the 1 April 1918; the establishment of the USAF was authorized on 26 July 1947 by President Harry S Truman, under Section 208 of the National Security Act and began operating on the 18 September 1947.

[7] Builder employs the term Icarus Syndrome to describe "a crisis of values in the USAF." This crisis is argued to exist because of a fundamental abandonment of guiding air power theory. Builder, *The Icarus Syndrome*, xviii.

[8] Builder, *The Icarus Syndrome*, xvii.

[9] Advocates such as Arquilla promise cyber-facilitated victory at low cost in terms of both blood and treasure. See John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review* (Summer, 1994): 25.

information dominance must be replaced with the realities of *terra nullius* and the contemporary demands of the contested Fifth Battlespace.[10]

Is Cyber to be a Mere Alliance? The Cry for an Adequate Cyber Force

This thesis opened by paraphrasing Sir Winston Churchill's reflections on air power, positing that not to have an adequate cyber force in the present state of the world would be to compromise the very foundations upon which our nations' freedoms rest. History's most tangible representation of adequate air power has been the creation of independent air forces. Consequently, authors such as Solce contest that if cyberspace's professionals-at-arms are to be allowed to aspire to become an adequate force, they too must be pushed from the nest by their elder services and allowed to fly as an independent "Cyber Force."[11] This argument is not confined to the realm of academia. For example, General Schwarz reflected that the development of a "new warfighting domain usually generated the requirements for new organizations" and specifically cited the formation of the USAF from the Army Air Service, and Army Air Corps.[12] Indeed, General Schwarz also posed the question: "Is cyber to be a mere alliance of many separate parts?"[13] The contemporary Fifth Battlespace, like air in its formative militarized years, represents an imperfect commons of competing ownership claims of many separate parts.[14] It is perhaps understandable, therefore, that air power's past casts its shadow over cyber power's future, and paints a picture of a strategic landscape plagued by the friction and frustrations inherent in operating as a mere alliance, ever deficient in terms of well defined boundaries and rules.

---

[10] *Terra nullius* is a Latin expression that means "no man's land."

[11] Natasha Solce, "The Battlefield of Cyberspace: The Inevitable New Military Branch, " Albany Law Journal of Science and Technology, no.293 (2008). http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/albnyst18&div=11&id=&page= (accessed 20 January 2011).

[12] General Norman Schwarz, Chief of Staff, US Air Force, Address. "The Challenge of Cyberspace", 27 October 2010, 7. http://www.af.mil/shared/media/document/afd-101102-046.pdf. (accessed 10 November 2010).

[13] Paraphrased from President Eisenhower regarding the formation of NATO as greater than the sum of its constituent nations.

[14] The metaphor is drawn from *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: Center for Strategic International Studies, 2008).

Analogical reasoning should not therefore be overly criticized for extrapolating such comments to prematurely reach the conclusion that an independent Cyber Force is both inevitable and operationally beneficial. But this thesis' employ of Khong's AE Framework at the micro-level provides a safety net to protect against such illogical leaps of faith. Step Three of Khong's model demands that a range of potential solutions should always be sought.[15] Thus, whilst a single independent Cyber Force would meet the demands of the Fifth Battlespace, so too does the current US construct of Service-specific cyber-oriented units providing force elements at readiness to a Joint overarching organization: the sub-unified command, US CYBERCOM. An analysis of the perils that exist in these competing organizational constructs is therefore warranted if cyber power is to truly reap the benefits of analogical reasoning.

The Perils of an Independent Cyber Force

As Gray notes, organizational issues are neither exciting, nor heroic, but they are a fundamental consideration if efficient and effective strategic performance is to be sought.[16] The "ends" of strategy may be achieved by the "ways" of tactics, but the mechanism to translate tactical activity to strategic effect is by "means" of the organization. The foundational building blocks for strategic performance are formed from an organization's processes; prioritization; planning; and provision of domain-oriented professionals-at-arms. The independent organizational form that air power assumed was therefore not simply because war had been elevated to the third domain, but rather to meet the demands of war-fighting in a new domain. Demands that many at the highest levels of government believed that the Army and Navy were failing to meet: "either through lack of vision, lack of practical knowledge, or deliberate intention to subordinate the Air Service… the Army has utterly failed to appreciate the full value of this military weapon and, in my opinion, has utterly failed to accord it its just place in our military family."[17] It would take almost three decades before Foulois' dream of air power being raised to sibling status in the military family was eventually realized in the formation of the USAF.

---

[15] Khong, *Analogies at War*, 22.

[16] Gray, *Modern Strategy*, 34.

[17] Quote taken from General Foulois' testimony before Congress in 1919. Army Reorganization: Hearings before the Committee on Military Affairs, House of Representatives (Washington, 1919), 932.

The path to air power's independence was not taken lightly on either side of the Atlantic. As General Patrick noted: "the Air Service…has probably been the most investigated activity ever carried on by the United States."[18] History supports Patrick's assertion. By 1934, over fourteen studies had been conducted to consider the formation of an independent air force. Many more assessments would follow before air power finally escaped, rather than was pushed, from the nest of its sister services.[19] The danger in Patrick's comment is that the volume of analysis conducted does not necessarily relate to the degree of intellectual rigor contained therein. Indeed, as Craven and Cate note, the formation of an independent air force can be argued to represent a uniquely polarized *cause célèbre* in military history, characterized more by the widespread employ of Fabian tactics than analytical impartiality.[20]

Paralysis by analysis is perhaps too strong a term for the inertia that these studies introduced, but they do highlight the consequences that Allison and Zelikow's Model II of bureaucratic politics can have if such bureaucratic norms are left unchecked. Model II organizational behavior is typified by the demonstration of marginal and incremental adaptation due to bargaining processes aimed at maximizing each sub-unit's own advantage, whilst at the same time inhibiting any change that could be detrimental to themselves.[21] Most importantly for the purposes of this thesis, Model II behavior is also characterized by imperialism: an organization's central goal of health being defined not by its development of more efficient and effective capability; instead, organizational health becomes synonymous with maintaining or attaining its autonomy.[22] As *Autonomy of the Air Arm* concludes, by 1947 air power had already reached an equivalent status to its land and maritime domains in terms of delivering military effect. Consequently, the formation of the USAF, rather than serving to meet the demands of developing a new military profession-at-arms to conduct battle in the third dimension, was instead more

---

[18] Quoted in Craven and Cate, *The Army Air Forces in World War II: Volume 1, Plans and Early Operations January 1939 to August 1942* (Chicago: University of Chicago Press, 1948), 22.
[19] For an outstanding summary of these investigations, see Craven and Cite, *The Army Air Forces in World War II: Volume 1, Plans and Early Operations January 1939 to August 1942,* 17-71.
[20] Craven and Cate, *The Army Air Forces in World War II: Volume 1, Plans and Early Operations January 1939 to August 1942,* 21-23.
[21] Graham Allison and Philip Zelikow, *The Essence of Decision: Explaining the Cuban Missile Crisis* (New York, NY: Longman, 1999), 143-185.
[22] Allison, *The Essence of Decision: Explaining the Cuban Missile Crisis*, 181.

justified on the imperialist grounds of providing parity in the political battlespace. Air power was presented as the political victim of ongoing internecine defense rivalries that had resulted in "no well defined habits of collective action or co-ordination:" only independence could serve as the cure.[23]

This thesis therefore contests that the ultimate victim of air power's "poorly defined habits of collective action and co-ordination" was actually its own peacetime military innovation: not how to most efficiently organize one's forces whilst fighting the current war; but rather how to build and prepare one's forces to fight future wars. As Rosen argues, if a military organization is healthy, there is no permanent norm defining the dominant professional activities of the organization.[24] Instead, many theories akin to the previous chapter's Slessorian and Douhetian paradigms are allowed to co-exist. Each theory presents a differing perception of the relative priorities of a battlespace's roles and missions, and serves to inform a dynamic debate that challenges basic assumptions in a manner that is non-threatening to the organization's autonomy. As has already been presented, a well-founded taxonomy of the competing roles and missions is therefore essential. But this taxonomy will be to no avail if competing theories are not in place to assess their relative import in the contemporary context. A healthy cyber organizational construct is therefore an essential nurturing factor if the development of cyber power is to be achieved. In contrast, this argument contests that the Athena Syndrome only serves to stifle the innovation that is so essential to the well-rounded growth of cyber power and cyber professionals-at-arms.

Rosen's analysis of the development of air power leading up to, and within World War II, serves to demonstrate that if senior military leaders wish to formulate creative strategies that can be effectively married to the contemporary security context, they must have both an intellectual and organizational framework in place to support such an aspiration: a deficit in either facet will lead to the stifling of innovation.[25] But an organization striving to secure or retain independence is more likely to espouse a dominant and unifying operational norm. This, in turn, rigidly bounds the professional activities of the organization and stifles innovation in so doing. As the Lampert

[23] R Earl McClendon, *Autonomy of the Air Arm* (Montgomery, AL: Air University, 1996), 107-108.
[24] Rosen, *Winning the Next War,* 19.
[25] Rosen, *Winning the Next War,* 21.

Committee recorded, the issue of air power's independence did indeed become all-consuming: "[Independence] has been discussed everywhere I have been where there are any Air Service officers and I have never heard anybody yet - any Air Service officer - against it."[26] As Allison's Model II behavior predicts, organizational independence became synonymous with operational autonomy and an overly polarized emphasis upon the norm of air power's deep strike role.[27] Air power employed in an auxiliary role was hence perceived in a pejorative sense. Imperialist tendencies favored roles that supported air power's quest for independence, to the detriment of developing its auxiliary capabilities.[28] This thesis posits that air power's quest for independence demonstrates the perils of the Athena Syndrome: independence becomes a most dangerous self-serving prophecy. Auxiliary roles such as Van Creveld's "directed telescope";[29] the "long arm" of air mobility;[30] and counter-land, counter-sea, and information operations, by not providing an autonomous function for air power advocates, are lost in the failing peripheral vision of those infected. Instead, the "logic of autonomy" demands that air advocates bias the pursuit of capabilities that directly promote their perceived key metric of organizational health: independence.[31] Like the Pathfinders' flares, strategic bombing would serve to illuminate air power's path to its target of becoming a separate service.[32]

Military cyber power, like military air power, lives in a bureaucratic world akin to Allison's Model II organization. Thus, if cyber power is not to sell its soul of developing a wide-fronted professionalism-at-arms, free to draw from the best of opposing paradigmatic schools of thought, the temptation of an imperialist cure-all must be resisted. A key lesson for cyber's taxonomy is therefore that reference to cyber power as

---

[26] Lampert Committee Hearing, *Inquiry into Operations of the U.S. Air Services: Hearing before Select Committee of Inquiry into Operations of the U.S. Air Service, House of Representatives* (Washington, 1925), 2240.

[27] For example see the wording in the Air Corps Act which explicitly states that the Act's aim is to "strengthen the conception of military aviation as an offensive, striking arm rather than an auxiliary service." The US Army *Air Corps Act of 1926*, http://www.airforcehistory.hq.af.mil/PopTopics/aircorpsact.htm (accessed 3 March 2011).

[28] Perry Smith, *The Air Force Plans for Peace, 1943-1945* (Baltimore: Johns Hopkins Press, 1970), 35.

[29] Van Creveld, *Command in War*, 75.

[30] Probert, *The Forgotten Air Force: The Royal Air Force in the War Against Japan, 1941-1945,* 194.

[31] The term "logic of autonomy" is coined by Richard Jensen, *Information War Power: Lessons from Air Power*, (Cambridge, MA: Program of Information Resources Policy, 1997), 70.

[32] Randall T Wakelam, *The Science of Bombing: Operational Research in the RAF Bomber Command* (Toronto: University of Toronto Press, 2009), 193-194.

an independent war winning capability must consciously be barred from its lexicon if the risk of stifling organizational innovation is to be averted.[33] Moreover, to promote a healthy organizational culture that is not threatened by competing military theories, references to cyber power in an auxiliary or supporting function must be celebrated rather than shunned.

An important second-order conclusion that this reflection highlights is that healthy change cannot be brought about by mavericks. Cyber power is not best served by a modern-day Mitchell, or leaders of a Douhetian bent and candor. Model II organizations tend to evolve incrementally, rather than by dramatically re-engineering their processes and priorities overnight. This demands that cyber leaders are cognizant and comfortable with the temporal nature of leading a Model II organization: continuity of effort and vision is demanded in those seeking to change the system. Mavericks, by their very definition, operate outside the confine of the system, and in so doing neglect the calculations of bureaucratic feasibility.[34] Hence, they do not have the longevity or sustained political support to bring about effective change over a prolonged period of time. The rallying cries of cyber power's Mitchells and Douhets must hence be muted. Advocacy founded upon calls for independence must be balanced by an awareness of the perils inherent in such a path if innovation in the Fifth Battlespace is not to be quashed.

But it is equally important not to misconstrue this thesis' counsel to believe that cyber power must be passive and accept the bureaucratic bonds that restrict a Model II organization. Radical change can be achieved on rare occasions: at times of budgetary feast; or after dramatic operational failings.[35] Taking advantage of these windows of opportunity is the *coup d'oeil* that cyber's leaders must possess.[36] The folly of mavericks is that vision, without trust both within the organization and amongst political leaders, will rarely bring about the great change they themselves demand.

An Alternative Mechanism for Creating Well Defined Habits…

[33] For an interesting parallel debate that has been presented regarding contemporary air power thinking see Mark Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*, (Lincoln, NE: University of Nebraska Press, 2006), 211-223.

[34] For the purposes of this thesis, a maverick is defined as "an outsider who may have brilliant ideas but who has rejected the system and has been rejected by the system."

[35] Allison, *The Essence of Decision: Explaining the Cuban Missile Crisis*, 171-172.

[36] *Coup d'oeil* is a French term that translates to "glimpse" or more literally "the stroke of the eye". Clausewitz coined the term in his consideration of the genius of the commander. Clausewitz, *On War*, 102.

Advocates for an independent cyber service may counter the arguments presented in the last section by striking their own historic analogy, specifically citing the RAF's experience leading up to the Battle of Britain. Young writes that whilst the planning of air defense was not a major priority of the RAF policy in the inter-war era, an independent organizational framework allowed competing theories of air power to facilitate the evolution of Dowding's air defense system of systems that proved so vital to operational-level success.[37] The RAF's early release from the shackles of pursuing independence can therefore be framed as the primary enabler of a safe, dynamic environment that was conducive to innovation. Conti and Surdu demand the adoption of a similar path for cyber's development. They contest that it is time for a cyberwarfare branch of the military, positing that technological advances have driven fundamental changes to how warfare is conducted.[38] Existing military organizations, accused by Conti of being technically and culturally inadequate to deal with this radical change to cyber's professionalism-at-arms, are thus shunned in favor of the path of independence.[39]

But such an argument confuses independence with autonomy. Dowding's system of systems did indeed facilitate success in the Battle of Britain. But this thesis contests that success was achieved by coupling a thorough understanding of the evolving technical realities of the fighting in air domain; with autonomy of action to effect such change. The Battle of Britain therefore represents not a rallying cry for independence, but rather Rosen's facets of peacetime innovation: the marrying of an intellectual and organizational framework that can best meet the needs of a rapidly changing environment.[40]

Cyberspace has been defined in this thesis as: *"…for the purpose of creating effects in cyberspace or its sister domains: land, sea, air and space."* A significant flaw in Conti and Surdu's logic is that their analysis assumes that an independent cyber force will be best placed to understand the creation of effects in cyberspace's sister domains. This thesis contests that Dowding's system of systems was effective because it coupled

[37] Neil Young, "British Home Air Defence Planning in the 1920s," *Journal of Strategic Studies,* (December 1988): 507.
[38] Gregory Conti and John Surdu, "Army, Navy, Air Force, and Cyber – Is it Time for a Cyberwarfare Branch of the Military?" *IA Newsletter,* Vol 12, no.1 (Spring 2009).
[39] Conti, "*Army, Navy, Air Force, and Cyber – Is it Time for a Cyberwarfare Branch of the Military?"* 16.
[40] Rosen, *Winning the Next War,* 21.

an expertise in achieving an effect in the air domain, with an understanding of the evolving technical realities of that domain. History therefore suggests that cyber power, if it is to support the creation of effects in its sister domains, must harness the expertise of those who create effects in the land, maritime, air and space domains; with a technical understanding of the role that cyber power is playing to support the creation of those effects. As eluded to in Chapter One, this task is in hand: the Navy has re-established the Tenth Fleet; the USAF is positioning itself to fight and win in cyberspace with the creation of the Twenty-fourth Air Force; and the Second US Army has answered the cyber call-to-arms. Each Service has therefore married its means of achieving military effect within its primary battlespace, with a technical understanding of the demands of the cyber domain.[41] The danger to date in this approach is that each Service has developed its capabilities in relative isolation, and like air power in its formative years, this has been an inherently non-linear, and bottom-up process. A means of creating well defined habits of collective action and co-ordination is thus required if the cries for cyber independence are to be muted: this is the realm of a Joint organization like US CYBERCOM.

Cyber power is indeed an imperfect commons of competing ownership claims; however, one advantage of allowing the Services relative autonomy in assuming responsibility for protecting and facilitating their own layers of cyberspace, and their service-specific roles and missions, is that it also helps better define *terra nullius*: those contested facets of cyberspace where no extant organization has sole responsibility; and just as importantly, the no man's land of cyberspace where no organization currently assumes responsibility. This is the battlespace of the Joint cyber organization.

But an acknowledged risk of such a system is that domain-oriented Services can, all too easily, become domain-fixated. Rosen, reflecting upon the efficacy of RAF Bomber Command's sustained strategy of area-bombing German cities, notes that processes adopted early-on can become "locked in place," despite subsequent experience.[42] Thus, innovation may be blocked after an all-too-brief period of experimentation. But as Gray notes, organizations also offer the potential benefit of

[41] Clarke, "*War from Cyberspace*," 33-44.
[42] Rosen, *Winning the Next War*, 26-27.

crafting "institutional safeguards that can help offset individual failings."[43] A further role of US CYBERCOM is therefore to act as an organizational screen against the symptoms of the Athena Syndrome and ensure that evolving cyber power theory is not subordinated to the execution of any Service's locked-in primary mission.[44] Whilst it is each Service cyber sub-unit's role to be domain-oriented, it is the Joint organization's responsibility to ensure that each cyber sub-unit does not become domain-fixated. But this dynamic is also bi-directional, and it is equally important for the Service cyber-components to ensure that the Joint organization also does not succumb to the maverick's siren song of independence.

US CYBERCOM can therefore be presented as fulfilling a moderating function for a Model II cyber organization. Its role is to balance the needs of Builder's "heart and soul": the heart that is cyber power writ large, must remain strong, exercised by the dynamic of balancing competing cyber theories, roles and missions; the soul of cyber power is the nurturing of each Service's cyber professionals-at-arms, as well as those cyber professional-at-arm functions, such as deep strike, that span the fuzzy boundaries of cyberspace. A Joint cyber organization thus satisfies General Schwarz's challenge: cyber power is no mere alliance of bottom-up capabilities, but instead represents a means of promoting Rosen's organizational health by ensuring no single, permanent norm defines the dominant professional activities of the organization.[45] Many competing paradigms are not only allowed, but are actively encouraged to co-exist, as long as each is articulated in the common language of a centrally defined cyber taxonomy.

Conclusions

Libicki and Hazlett wrote that: "When it comes to radical re-organization, and forming a [Cyber Force] certainly qualifies, a first rule of thumb may be: when in doubt, don't."[46] Analysis by means of Gray's organizational dimension of strategy, coupled

[43] Gray, *Modern Strategy*, 33.
[44] Builder, *The Icarus Syndrome*, xviii.
[45] Rosen, *Winning the Next War,* 19.
[46] The exact term used by Libicki and Hazlett was Information Corps rather than Cyber Force; however, the thrust of their argument is that an information force would be required to develop doctrine, weapons and employment concepts, independent of the existing Services. To that end, their concept is closely aligned to this thesis' consideration of an independent cyber force.

with Khong's historical analogy framework, has served to expose numerous doubts and risks that caution against following in air power's footsteps. This thesis has argued that lazy analogical reasoning regarding air power's quest for independence carries with it a significant risk of cyber power succumbing to the Athena Syndrome: tunnel-vision that can lure cyber power's leadership off of the path of strategic efficacy; and blind them to the pitfalls that lie in wait on the path to organizational independence.

Military cyber power, like military air power, has been presented as existing in the bureaucratic reality of Allison's Model II organization. The risk herein is that unchecked imperialism may result in cyber power failing to develop a broad-fronted professionalism-at-arms; and a culture that cannot draw from the best of opposing paradigmatic schools of thought. A key lesson for cyber power's taxonomy is therefore that reference to cyber power as an independent war winning capability must consciously be barred from its lexicon if the risk of stifling organizational innovation is to be averted. Moreover, to promote a healthy organizational culture that does not suppress competing theories of cyber power, cyber's auxiliary functions must be celebrated, rather than subordinated as unwelcome diversions from the path to independence.

As Gray argues, "It is a general rule that combined arms are stronger than single arms."[47] This thesis has suggested that a Joint cyber organization that corrals the efforts of single service cyber units represents a most adequate means of creating well-defined habits of collective action and co-ordination; whilst also serving to help define the imperfect commons that is cyberspace. Such a mechanism grants each Service relative autonomy to assume responsibility for protecting and facilitating its own layers of cyberspace, service-specific roles, and missions. In so doing, this also serves to help better define *terra nullius*: the contested facets of cyberspace where no single

---

An excellent further point of note that Libicki and Hazlett proffer is that that whilst the USAF was forged from the Army Air Service, a Cyber Force would have to be formed from all of its sibling services and "by taking from all, it would be opposed by all." This thesis' analysis has emphasized that air power's intellectual founding fathers sought to garner interest and investment for air power in a period of harsh fiscal climes, and in the face of stiff organizational resistance from the extant military services. If Libicki and Hazlett's excellent argument is accepted, the institutional resistance and friction that creation of an independent Cyber Force would generate is likely to exceed that of the formation of independent air forces. See Martin Libicki and James Hazlett, "Do We Need an Information Corps," *Joint Forces Quarterly*, no.2 (Autumn 1993): 97.

[47] Colin Gray, *Explorations in Strategy* (Westport, CT: Praeger, 1998), 125-134.

organization has responsibility; and the no man's lands of cyberspace where no organization currently assumes responsibility. Whilst each Service cyber unit can remain domain-oriented, the Joint organization can ensure that each cyber sub-unit does not become domain-fixated. This dynamic has also been presented as being bi-directional, so that each Service cyber sub-unit can help protect against the Joint organization from succumbing to the maverick's siren song of independence. A cyber organization of this form thus becomes a symbiotic whole: cyber power is one piece; a broad-fronted cyber professionalism-at-arms is the other. Both heart and soul are nurtured, and in so doing, the risk of the Athena Syndrome is mitigated.

CONCLUSION

There are lies, damn lies, and…

-- Charles W. Dilke

If Anthony Eden were alive today, he may well concur that: "There are lies, damn lies, and the lessons of historical analogy!" Analogy is a flattering mistress who will whisper any sweet nothing that one wishes to hear. The consequences of acting upon such honeyed historical lessons can be disastrous, as Britain's least successful prime minister would surely attest to. The challenge for those who wish to look back, in order to move forward is to ensure that the dangers of lazy analogy are keenly avoided.

The thesis has dared to look back at the hard-earned, and oft bitter, lessons of air power's experience in an effort to help cyber power move forward, more cognizant of the pitfalls that may lie in wait upon its path. The guides on this perilous analysis have been sure: Gray and Khong have provided a methodological screen through which the history of air power's operational, theoretical, and organizational dimensions have safely been observed. Whilst it has been shown that air power's evolution cannot be employed as a map to chart cyber power's future path, it has been demonstrated that air power's rich experience can serve as a guide for the more expedient, efficient and effective development of cyber power.

The prism of air power has been applied to cyber power and a spectrum of cyber roles, far more glorious in color and depth than their dull contemporary equivalents of CNA, CNE and CND, has been exposed. A coherent and demystified cyber lexicon has been proposed. A lexicon that includes more complete definitions for cyberspace and cyber power, beneath which sit a Clausewitzian triumvirate of roles: ISR; cyber attack; and control of cyberspace. Within each of these roles, subordinate cyber missions have been identified. It has been proposed that cyber-borne ISR, as well as providing support to cyber's sibling domains, also comprises the Janus-faced missions of JIPCE (Friendly) and JIPCE (Enemy). With regard to cyber attack, the roles of deep attack; counter-land; counter-sea; counter-air; and information operations have all been demonstrated to have applicability. Last, the core cyber function, control of cyberspace, was identified and a

case presented to support the need for offensive and defensive counter-cyber operations. Furthermore, the extant terms CNA, CND and CNE have been charged as being nothing more than legacies of a by-gone paradigm, serving only to cognitively blur cyberspace's already fuzzy borders. But this study's lexicon is by no means complete: air power's experience can only serve as a springboard for the development of cyber power's taxonomy, and future inductive study is this area is recommended.

This thesis then turned its analytical focus upon two broad paradigmatic schools of air power theory: a Douhetian paradigm; and a Slessorian school of thought. Analysis of the Douhetian paradigm exposed numerous lessons that any future cyber power strategy should seek to assimilate. First, the author has contested that the offensive dominance of cyber power's character cannot be assumed: future offensive military capability does not follow Moore's Law and cannot be extrapolated from the limited capabilities currently demonstrated. Second, a risk of strategic over-expectancy has been exposed: built upon an unfounded faith in the existence of panacea industrial or economic cyber targets; or the erroneous assumption that the will of an Information Age populace can be fashioned into a cyber-assailable center of gravity. If the firestorms of Dresden could not crush the spirit or economy of the German people, even the most all-encompassing cyber assault is unlikely to break the bank, or the will, of the UK or US. Coupled with these lessons, the cyber skirmishes of Estonia, Georgia, and Iran have all potentially served to validate a growing perception that civilian and industrial infrastructure represents a legitimate military target in any future cyber conflict. A pitfall of the ethically questionable use of cyber power has thus been highlighted and presented as a very real risk that only cyber's military leaders are positioned to protect against.

In considering the pertinent lessons to be drawn from the Slessorian school of thought, this thesis has emphatically challenged any digital Douhetian who asserts that "If you are defending in cyberspace, you're already too late."[360] Siena's cyber walls will not fail because they are, on occasion, breached. A paradox of cyber power is that cyber defenses will fail if they are built too securely, or hidden behind for too long. Cyber power's leadership must hence emphasize to their professionals-at-arms that delivery of military success in cyberspace ultimately rests on the facilitation of its information-

[360] Clarke, *Cyber War: The Next Threat to National Security and What to Do About It*, 36.

enabled sibling services in the physical domain. In turn, the Faustian bargain those seeking to develop cyber-enabled forces must resist, is that of becoming overly transformational because the price of excessively leveraging cyber power could well be the surrendering of one's own cyber integrity. Consequently, analysis of Gray's strategic dimension of theory concluded that that any surrogate theory of cyber power must support a balanced cyber portfolio, albeit with an emphasis placed upon control of cyber space as the *primus inter pares* of cyber's missions.

The ultimate peril of air power's competing paradigms has been cast as the danger of seeking to fill cyber power's current theoretical void with a single absolute akin to Starr's cry for a unitary, comprehensive and robust theory.[361] A degree of ambiguity, whilst unsatisfying to strategists seeking topiary perfection in Clausewitz's "hedges of principles," has been shown to better serve cyber power's contemporary guiding needs if the Athena Syndrome is to be averted. Indeed, this thesis has argued that the premier indicator of a healthy military cyber organization is the existence of a culture that has no permanent norm defining its dominant professional character. An organizational construct that draws upon the expertise of cyber's sibling services therefore serves as a welcome inoculation against the siren song of independence, and the misplaced advocacy of would-be cyber mavericks.

Finally, this thesis has argued that Jointery, in the form of a central cyber organization, empowered to corral the efforts of these single-Service cyber elements, represents an effective means of creating well-defined habits of collective action and co-ordination. As well as creating a symbiotic organizational whole that promotes the development of both central cyber power, and a broader cyber professionalism-at-arms, such a construct also serves to help better define *terra nullius*: the contested facets of military cyberspace where no single organization has responsibility; and the no man's lands of cyberspace where no organization currently assumes responsibility.

Most importantly, this thesis acknowledges that its employ of analogical reasoning acknowledges is incomplete. This has been deliberately so. The lessons exposed in this study are crafted to serve as nothing more than a brief expedient; to help cyber power confront its most immediate challenges and needs and create a degree of

[361] Starr, *Toward a Preliminary Theory of Cyberpower,* 44.

control over the emergent and bottom-up process that has frustrated cyber power's coherent development to date. But analogical reasoning has limited utility with regard to anticipatory value: it can highlight pitfalls, but it can never chart the best course for the evolution of the Fifth Battlespace. Not to have an adequate cyber force would be to compromise the foundations on which our freedoms rest. This thesis may serve to help satisfy Churchill's call for adequacy. For a more complete theory of cyber power, inductive reasoning, and the analytical extrapolation of cyber's ever-burgeoning history, must guide the way from adequacy to excellence.

BIBLIOGRAPHY

Abbott, Andrew, *The System of Professions: An Essay of the Division of Labour*, Chicago, IL: University of Chicago Press, 1988.

Ackoff, Russell, "Towards a System of Systems Concept," *Management Science*, Vol 17, no. 11, July 1971.

Adams, James, "Virtual Defense," *Foreign Affairs*, May/June 2001.

Air Publication 3000 Edition 4, 2009.

Air University. *Style and Author Guide*. Maxwell AFB, AL: Air University Press, 2005.

Alberts, David and Hayes, Richard, *Power to the Edge : Command and Control in the Information Age*, Washington, DC: Command and Control Research Program, 2003.

Alberts, David, Gartska, John and Stein, Frederick, *Network-Centric Warfare. Developing and Leveraging Information Superiority*, Washington D.C.: Library of Congress, 1999.

Alford, Lionel, "Cyber Warfare: The Threat to Weapon Systems," *WSTIAC Quarterly*, Vol 9, no.4, Winter, 2009.

Allison, Graham T. and Zelikow, Philip D. *Essence of Decision: Explaining the Cuban Missile Crisis*. New York: Longman, 1999.

Arquilla, John and Ronfeldt, David, In Athena's Camp: Preparing for War in the Information Age, Santa Monica, CA: RAND, 1997.

Arquilla, John, "The Strategic Implications of Information Dominance," *Strategic Review*, Vol 22, no.3, Summer 1994.

Michael F Beech, *Observing Al Quaeda Through the Lens of Complexity Theory: Recommendations for the National Strategy to Defeat Terrorism*, Centre for Strategic Leadership, US Army War College, July 2004.

Baldwin, Stanley, *House of Commons Debates*, 10 November 1932, Vol 270.

Baring, Maurice, *R.F.C H.Q. 1914-1918*, London: Bell, 1920.

Barlow, Jeffrey, *Revolt of the Admirals*, Washington D.C.: Naval Historical Center, 1994.

Beyerchen, Alan. *Clausewitz, Non-linearity and the Unpredictability of War*. "International Security. 17 (1992/1993): 59-90.

Biddle, Tami Davis, *Rhetoric and Reality in Air Warfare: the Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, Princeton, N.J. ; Woodstock: Princeton University Press, 2004.

Beagle, T.W., *Effects-Based Targeteting: Another Empty Promise?* Air University, June 2000.

Bijker, Wiebe E., et al, *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1989.

Blank, Stephen, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy*, Vol 27, Issue 3, May 2008 , 227–247.

Briscoe, Bob, "Metcalfe's Law is Wrong," *IEEE Spectrum*, July 2006.

Bousquet, Antoine, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, New York: Columbia University Press, 2009.

British Bombing Survey, Effects on German Towns.

Brown, Michael "Information Warfare and the Revolution in Military Affairs", *Seminar on Intelligence, Command, and Control, Guest Presentations*, Spring 1995.

Builder, Carl, *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and Fate of the U.S. Air Force*, New Brunswick, NJ: Transaction Publishers, 2009.

Bungay, Stephen, *The Most Dangerous Enemy: an Illustrated History of the Battle of Britain*, Minneapolis: Zenith Press, 2010.

Bunker, Robert, *Five-Dimensional (Cyber) Warfighting: Can the Army After Next Be Defeated Through Complex Concepts and Technologies?* March 1998.

Cashell, Brian, Jackson, William D., Jickling, Mark, and Webel, Baird, *The Economic Impact of Cyber-Attacks*, 1 April 2004.

Carlin, John, "A Farewell to Arms," *Wired*, May 1997.

Cebrowski, Arthur, and Garstka, John, "Network-Centric Warfare: Its Origin and Future", *Proceedings*, US Naval Institute, January 1998.

Checkland, Peter, *Systems Thinking, Systems Practice*. New York, NY: Wiley, 1999.

Clausewitz, Carl von. *On War*. trans. and ed. Michael Howard and Peter Paret. Princeton: Princeton University Press, 1984.

Clarke, Richard, *Cyber War, The Next Threat to National Security and What to Do About It*, New York: Ecco, 2010.

Clarke, Richard, "War from Cyberspace,*" The National Interest,* November-December 2009.

Clayton, Mark, "Stuxnet Malware is Weapon," *Christian Science Monitor*, http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant

Clodfelter, Mark, *The Limits of Air Power: The American Bombing of North Vietnam*. Lincoln, NE: University of Nebraska Press, 2006.

Collins, Brian, *Behind the Cyberspace Veil, The Hidden Evolution of the Air Force Officer Corps*, Westport, CT: Praeger, 2008.

Conti Gregory, and Surdu, John, "Army, Navy, Air Force, and Cyber – Is it Time for a Cyberwarfare Branch of the Military?" *IA Newsletter*, Vol 12, no.1 Spring 2009.

Cohen, Elliot, "The Future of Force," *The National Interest*, Autumn 1990.

Cornish, Paul, *On Cyber Warfare*, London: Chatham House, 2010.

Craven W.F. and Cate J.L., *The Army Air Forces in World War II: Volume 1, Plans and Early Operations January 1939 to August 1942*, Chicago: University of Chicago Press, 1948.

De Groot, Gerard, *The Bomb: A Life*, Cambridge, MA: Harvard, 2005.
Denmark, Abraham, "Managing the Global Commons," *The Washington Quarterly*, 33:3.
Denning, Dorothy, *Information Warfare and Security*, New York, NY: ACM Press, 1999.
Dolman, Everett. *Astropolitik: Classical Geopolitics in the Space Age.* London: Cass, 2006.
Dolman, Everett, *Pure Strategy: Power and Principle in the Space and Information Age*. New York, NY: Cass, 2005.
Douhet, Giulio, *The Command of the Air,* Tuscaloosa, AL: University of Alabama Pres, 1998.
Eden, Anthony, *Full Circle*, Boston, MA: Houghton Mifflin, 1960.
Emme, *The Impact of Air Power*, Princeton: Van Nostrand, 1959.
Farwell, James, "Stuxnet and the Future of Cyber War," *Survival*, Vol 53, No 1, February-March 2011.
Fischer, David, Hackett, *Historians' Fallacies: Toward a Logic of Historical Thought,* New York: Harper Torchbooks, 1970.
Fredette, Raymond, *The Sky of Fire: The First Battle of Britain 1917-1918 and the Birth of the Royal Air Force*, New York: Holt, Rinehart and Winston, 1996.
Fuller, J.F.C. *The Foundations of the Science of War*, London: Hutchinson & Co., 1926.
Gates, Robert, "A Balanced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs*, January / February 2009.
Gould Lee, Arthur, *No Parachute: A Fighter Pilot in World War I; Letters Written in 1917 by A. S. G. Lee*, New York, NY: Harper & Row, 1970.
Gould, Stephen, Jay, *Rocks of Ages: Science and Religion in the Fullness of Life*, New York: Ballantine, 1999.
Grant, Rebecca, *Victory in Cyberspace*, http://www.afa.org/media/reports/victorycyberspace.pdf
Gray, Colin, *American Military Space Policy: Information Systems, Weapon Systems, and Arms Control*, Cambridge, MA: Abt Books, 1983.
Gray, Colin, *Explorations in Strategy,* Westport, CT: Praeger, 1998.
Gray, Colin, *Modern Strategy*. Oxford: Oxford University Press, 1999.
Hall, Wayne, *Stray Voltage: War in the Information Age*, Annapolis, MA: Naval Institute Press, 2003.
Howard, Michael, *The Causes of Wars and Other Essays*, London: Temple Smith, 1983.
Jakab, Peter L. *Visions of a Flying Machine: The Wright Brothers and the Process of Invention.* Washington: Smithsonian Institution Press, 1990.
James, Andrew, *Understanding Network Enabled Capability*, London: Ministry of Defence, 2009.
Jensen, Richard, *Information War Power: Lessons from Air Power,* Cambridge, MA: Program of Information Resources Policy, 1997.

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton: Princeton University Press, 1976.

Jervis, Robert. *System Effects: Complexity in Political and Social Life.* Princeton: Princeton University Press, 1997.

Johnson, Dana, *Roles and Missions for Conventionally Armed Heavy Bombers – A Historical Perspective*, Santa Monica, CA: RAND, 1994.

Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, 7 October 2004.

Joint Terminology for Cyberspace Operations, Memo from the Vice Chairman of the Joint Chiefs of Staff, General James Cartwright, 2010.

Kennet, Lee, *A History of Strategic Bombing*, New York, NY: Scribner, 1982.

Keymour, Eleanor, "The Cyber-war," *Jane's Defence Weekly*, 2009, Vol 47, Issue 39.

Kramer, Franklin, *Cyberpower and National Security* Washington, DC: National Defense University Press: Potomac Books, 2009.

Khong, Yuen Foong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965.* Princeton: Princeton University Press, 1992.

Klein, John, *Space Warfare: Strategy, Principles and Policy*, New York, NY: Routledge, 2006.

Kolanda, Christopher , "Transforming How We Fight – A Conceptual Approach," *Naval War College Review*, Spring 2003.

Kuehl, Dan, *From Cyberspace to Cyberpower: Defining the Problem*, National Defense University Press, 2009.

Kuhn, Thomas S. *The Structure of Scientific Revolutions, Third Edition*. Chicago: University of Chicago, 1996.

Lambeth, Benjamin, *The Transformation of American Air Power*, Ithaca, NY: Cornell University Press, 2000.

Leiner, Barry et al, *A Brief History of the Internet*, http://www.isoc.org/internet/history/brief.shtml

Libicki, Martin, *Conquest in Cyberspace: National Security and Information Warfare*, New York, NY: Cambridge University Press, 2007.

Libicki, Martin, *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND, 2009.

Libicki, Martin, and Hazlett, James, "Do We Need an Information Corps," *Joint Forces Quarterly*, no.2, Autumn 1993.

Liddell Hart, Basil, *Strategy*, London: Faber & Faber, 1967.

Loader, Brian, *Cyberspace Divide: Equality, Agency and Policy in the Information Society* New York, NY: Routledge, 1998.

Lonsdale, David, *The Nature of War in the Information Age – Clausewitzian Future*, London; New York : Frank Cass, 2004.

Luttwak, Edward, "Economic Competition Will Replace Military Conflict: From Geopolitics to Geo-Economics," *National Interest*, Summer 1990.

MacAskill, Ewen, and Miller, Stuart, "America's Digital Division, the Biggest Advance in Warfare since the Tank," *The Guardian,* 7 April 2003.

MacIsaac, David, "The Air Force and Strategic Thought 1945 – 1951", Working Paper #8, *Woodrow Wilson International Center for Scholars*, International Security Studies Program, 1979

Mahan, Alfred Thayer, *The Influence of Sea Power on History (1660-1783),* Annapolis, MA, Naval Institute Press, 1991.

Mahnken, Thomas G. *Technology and the American Way of War.* New York: Columbia University Press, 2008.

Martin, Roger, *The Opposable Mind: Winning Through Integrative Thinking*. Boston, MA: Harvard Business Press, 2009.

May, Ernest, *Lessons of the Past; the Use and Misuse of History in American Foreign Policy*, New York, NY: Oxford University Press, 1973.

McClendon, R Earl, *Autonomy of the Air Arm*, Montgomery, AL: Air University, 1996.

McHugh, Paul, "Striving for Coherence: Psychiatry's Efforts Over Classification", *The Journal of American Medical Association*, no.293, 2005.

McInerney, Thomas, "'Stealth' Chinese Fighter Jet Photos No Accident," *Fox News*, 6 January 2011.

Michael, Alex, *Cyber Probing: The Politicisation of Virtual Attack*, London: Ministry of Defence, 2010.

Miller, Donald, *The Story of World War II*, New York, NY: Simon & Schuster, 2001.

Miller, Robert and Lachow, Irving, "Strategic Fragility: Infrastructure Protection and National Security in the Information Age." *Defense Horizons,* Center for Technology and National Security Policy, National Defense University, no. 59, January 2008.

Mitchell, William, *Winged Defense*, Tuscaloosa, AL: University of Alabama Press, 2009.

Molander, Roger C. *Strategic Information Warfare: A New Face of War,* Santa Monica, CA: RAND, 1996.

Mueller, Karl, *Air Power,* RAND, 2010.

Munro, Neil, *The Quick and the Dead: Electronic Combat and Modern Warfare*, New York, NY: St Martins Press, 1991.

Murphy, Dennis, "Attack or Defend? Leveraging Information and Balancing risk in Cyberspace", *Military Review*, May–June 2010.

Murphy, Dennis, "Talking the Talk: Why Warfighters Don't Understand Information Operations," *IO Journal*, Vol 1, no. 1, April 2009.

Nazario, Jose, *Georgia DDoS Attacks: A Quick Summary of Observations*
http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/

Nye, David, *American Technological Sublime*, Cambridge, MA: MIT Press, 1994.

Nye, Joseph, *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010.

Olsen, John Andrea, *John Warden and the Renaissance of American Air Power*, Washington D.C.: Potomac Books, 2007.

Omand, David, *Securing the State*, New York, NY: Columbia University Press, 2010.

Owens, William, Dam, Kenneth, and Lin, Herbert, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Committee on Offensive Information Warfare, Computer Science and Telecommunications Board, 2010.

Pape, Robert A. *Bombing to Win*, Ithaca: Cornell University Press, 1996.

Parker, Geoffrey, *The Military Revolution: Military Innovation and the Rise of the West, 1500-1800*, Cambridge: Cambridge University Press, 1996.

Posen, Barry. *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars.* Ithaca: Cornell University Press, 1986.

Probert, Henry, *The Forgotten Air Force: The Royal Air Force in the War Against Japan, 1941-1945*, London, Brassey's, 1995.

Pritchard, J. Laurence, *Sir George Cayley: The Inventor of the Aeroplane* ,London: Parrish, 1961.

Rattray, Greg, *Strategic* Warfare *in Cyberspace*, Boston, Mass: MIT, 2001.

Roman, Gregory, *The Command or Control Dilemma: When Technology and Organizational Orientation Collide*, April 1996.

Roodt, J. H. S., *Boundary Management and Integration Framework for a Joint Cyber Defence Capability for Military Forces: Analysis and Synthesis from a Through-Life Capability Management Perspective,* http://researchspace.csir.co.za/dspace/bitstream/10204/4848/1/Van%20Vuuren1_2010.pdf

Rosen, Stephen P. *Winning the Next War: Innovation and the Modern Military*. Ithaca: Cornell University Press, 1991.

Roskill, Stephen *The War at Sea, 1939-1945, Vol 3*, London: HMSO, 1961.

Ryan, Daniel and Ryan, Julie, Information Warfare, Thunder's Mouth Press, 1996.

Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Washington, D.C.: Center for Strategic International Studies, 2008.

Slabodkin, Gregory, "Navy CIO Orders an Investigation of Yorktown Systems Failure," http://www.cs.virginia edu/~survive/NEWS/news003.txt.

Slessor, John, *Air Power and Armies*, London: Oxford University Press, 1936.

Sheldon, John, *Reasoning by Strategic Analogy: Classical Strategic Thought and the Foundations of a Theory of Space Power*

Singer, P. W., *Wired for War*, New York: Penguin, 2009.

Smith, Merritt, and Marx, Leo, *Does Technology Drive History?: The Dilemma of Technological Determinism*, Cambridge, MA: MIT Press, 1994.

Smith, Michael, "General Sir David Richards Calls for New Cyber Army, *The Times*, 17 Jan 2010.

Smith, Perry, *The Air Force Plans for Peace, 1943-1945*, Baltimore: Johns Hopkins Press, 1970.

Solce, Natasha, "The Battlefield of Cyberspace: The Inevitable New Military Branch," Albany Law Journal of Science and Technology, no.293, 2008.

Spaight, James, *Aircraft in War*, London: MacMillan, 1914.

Sun Tzu, *The Illustrated Art of War*, Boston: Random House, 1998.

Talbot, Frederick, *Aëroplanes and Dirigibles of War*, London: Heinemann, 1915.

Tedder, Arthur, *Air Power in War* Tuscaloosa, AL: The University of Alabama Press, 2010.

Thompson, Kenneth, *Political Realism and the Crisis of World Politics*, Princeton, NJ: Princeton University Press, 1960.

Tikk, Eneken, *Cyber Attacks Against Georgia – Legal Lessons Identified*, CCDCOE, 2008.

Tobin, Scott, *Establishing a Cyber Warrior Force*, Ohio: Air Force Institute of Technology, 2004.

Toffler, Alvin, and Toffler, Heidi, *War and Anti-War: Survival at the Dawn of the 21st Century*, Boston: Little, Brown and Company, 1993.

Trias, Eric, and Bell, Bryan, *"Cyber This, Cyber That…So What?," Air & Space Power Journal*, Vol. 24, no. 1, Spring 2010.

Tsang, Rose, *Cyberthreats, Vulnerabilities and Attacks on SCADA Networks*, http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf

UK Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, London: Cabinet Office, 2010.

United States Strategic Bombing Survey (USSBS) Summary Report (European War).

US Air Force Doctrine Document 1, 17 November 2003.

US Federal Cybersecurity Market Forecast 2010-2015, *Market Research Media*, 5 May 2009, http://www.marketresearchmedia.com/2009/05/25/

Van Creveld, Martin, *Command in War*, Cambridge, Mass: Harvard University Press, 1985.

Van Creveld, Martin, *Technology and War*, New York: The Free Press, 1989.

Van Creveld, Martin, *Transformation of War*, New York: The Free Press, 1991.

Wakelam, Randall, *The Science of Bombing: Operational Research in RAF Bomber Command*, Toronto: University of Toronto Press, 2009.

Waldrop, M. Mitchell, *Complexity: the Emerging Science at the Edge of Order and Chaos*, New York : Simon & Schuster, 1992.

Waltz, Kenneth. *Theory of International Politics.* Boston: McGraw Hill, 1979.

Warden, John, *Employing Air Power in the Twenty-first Century*, Montgomery, AL, Air University Press, 1992.

Weigley, Russell, *The American Way of War: A History of US Military Strategy and Policy*, Bloomington: Indiana University Press, 1977.

Wells, H.G., *The War in the Air*, London, Penguin, 1907.

Winton, Harold *An Imperfect Jewel: Military Theory and the Military Profession*, Montgomery, Air University, 600 Reader.

Wynne, M.W., "Flying and Fighting in Cyberspace," *Air and Space Power Journal*, Vol. 21, no. 1, Spring 2007.

Young, Mark, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law & Policy*, Vol 4, no. 1, 2010.

Young, Neil, "British Home Air Defence Planning in the 1920s," *Journal of Strategic Studies*, December 1988.